FOCUS Health, Inc.
10801 Starkey Road, #104-101
Seminole FL 33777

POLICIES & PROCEDURES **TITLE: Security Policy & Procedure 15.0**

APPROVAL: Approved By:

12/10/2021	M. Bojkovic	1/20/2022	4/20/2021
Review Date	Michael Bojkovic, CEO	Effective Date	Revision Date

Table of Contents

Security Policies and Procedures Table of Contents

INTRODUCTION

FOCUS Health, Inc. (FH) is a virtual (decentralized) company; meaning our staff members are not centrally located in a traditional, centralized office setting. In order to facilitate business functions, FOCUS has created and deployed computer software on a platform of industry-standard computer hardware to provide access by stakeholders (client-companies, FOCUS employees and contracted Peer-Reviewers) for processing Reviews. By employing a model of distributed staff in multiple locations and leveraging technology to acquire, process and transmit information, it is critical that FOCUS maintains safeguards and data is accessed and processed only by approved personnel.

This document establishes FOCUS Health, Inc. (FH) Security Policy and Procedures. It provides methods for security policy development and implementation, assigns responsible management, and establishes procedures for security implementation and review, and resolution of security conflicts or incidents. FH's Review Management System, (an internally developed customized software solution which manages all FH data) is utilized by client-company care managers, FH staff members and FH Peer Reviewers. The sensitivity of information for all users of the system are considered equally critical.

Security Implementation Plan

The FH Chief Security Officer is to discuss security policy and procedures with supervisors. The CSO will specify the steps to be taken by each supervisor. The CSO and supervisors will review policies and procedures and raise concerns and issues for change and improvement to be taken into consideration. All security violations and non-compliance situations will be reported to the CSO. The CSO will work with the CEO, CMO and IT Staff to rectify these situations.

The following are specific actions and responsibilities:

- The CSO will discuss security on a regular basis at meetings with supervisors and staff.
- FH Security Policy & Procedure will cover computational security activities.
- Supervisors will keep their staff aware and informed of policies and procedures, and be responsible for security within their own area.
- Supervisors will make themselves available to discuss the FH Security Policy and Procedures document with each new employee. Employees are required to read this document and address any questions pertaining to it with their supervisor. Supervisors should review with each new employee the security policies and address security issues specific their role and responsibilities. This procedure is to be documented through the use of an electronic security document acknowledgment form that will be electronically signed by the employee and then made available to HR.
- HR staff will conduct an exit interview with a departing staff member prior to the staff member's final working day at FH. This interview will cover, among other things, a review of the non-disclosure agreements in effect for that person (if any have been signed). A discussion of the personal effects of the staff member will be made to attempt to identify any proprietary materials that may be among them and guard against such material leaving FH with the person. An employee exit form will be filled out and filed with the HR department.
- Security training sessions for staff will be conducted on a regular basis.
- Staff members will make visitors aware of FH's security policy and procedures where appropriate.

Establishing Policies and Procedures

The FH Chief Security Officer is be responsible for establishing applicable specific security policies and procedures. The FH CSO will conduct internal and external security reviews or audits in order to analyze, justify and revise current policies and procedures as applicable. The CSO will also be responsible for coordinating changes to security policy and procedures. A yearly assessment of the current policy and procedures document will be undertaken to assess whether any changes are required. Requests for changes will be reviewed by the FH CEO, CIO and CSO, who will review the feasibility and costs of the proposed changes. All changes in FH security policies and procedures will be approved by the CEO and CSO. The latest iteration of the FH Security Policy & Procedure document will be distributed to all FH staff members and FH peer reviewers responsible for carrying out the specific procedures.

FH's security policies and technical security architectures are designed to provide mechanisms whereby end users' access to data is sufficient to perform required tasks, but eliminates unnecessary exposure.

FH's security strategy is to provide staff with tools and education concerning security policy and procedures, relying on individuals to use this knowledge and these tools to implement security measures appropriate to their work. In addition, centralized security measures and controls are implemented to assure basic security and to provide administrative review of security.

It is the responsibility of each participating user, staff person, or client-company to use the tools available at FH to protect its assets and those of its staff, peer reviewers and client-companies from injury, theft, or unauthorized use. Primary security concerns for FH include:

- Protection of sensitive materials, including compliance with non-disclosure and other security related agreements. Each FH staff member and peer reviewer is required to read and sign such non-disclosure before accessing the system.

- Protection of the FH computing and information infrastructure including intellectual property (text, hardware, software, and data) stored or processed by the FH Review Management System.

MISSION STATEMENT

The FH Security Policy and corresponding security standards, guidelines or procedure documents have been developed to provide reliable protection of various FH assets. These assets may be resources (computational systems, printers and copiers), information (e.g., intellectual property), infrastructure (e.g., networks and facilities), or relationships (e.g., agreements with client-companies or peer reviewers).

Considered threats to these assets include—but are not limited to—direct cyber attacks from outsiders, improper resource use by employees and users, accidental disclosure of sensitive data, and natural or man-made disasters.

The role of FH is to:

(1) Educate users on how to properly handle sensitive information and use their computers in a security conscientious manner; and
(2) Support the central mission of the center by assuring confidentiality, integrity, and availability of its resources to its staff, client-companies and peer reviewers. In close collaboration with all stakeholders, FH helps protect our resources by focusing on assessing, detecting, and mitigating the risks to our network and computational systems.

This policy document establishes a baseline of policies, as well as, standards and procedures that apply to all FH staff members and peer reviewers in order to meet these goals. Furthermore, it is the responsibility of FH to maintain this document, update it and assist users in complying with it.

The scope of this policy and any corresponding documents are intended to be distributed to all individuals accessing the FH Review Management System, which includes (but is not limited to) FH staff members and FH peer reviewers.

AWARENESS

It is the policy of FH to provide an appropriate level of information security. All FH staff members and peer reviewers are required to read this document and take steps as needed to assure security. When security related questions arise they should be directed to the FH Security Officer.

Each staff member shall be provided with a copy of this FH Security Policy and Procedures document upon arrival to FH during the HR orientation process. It should be reviewed with his or her supervisor before being granted access to utilize the FH Review Management System. The general policies and procedures as well as the detailed procedures for the person's particular division and work should be reviewed. The briefing should cover all the sections of this document. The new employee must acknowledge that they have read and understand the security policy, and this will be documented with a security acknowledgement form to be signed by the employee. A paper original form may be kept in the employee's folder in Human Resources (HR), otherwise an electronic acknowledgement by the employee will be stored in a database accessible by HR and the FH Security Officer.

All new staff members are required to attend the new employee security training session. These sessions are held one-on-one with the FH Security Officer. The FH Security Officer, Chief Executive Officer and Chief Medical officer shall review the FH Security Policies & Procedures at least once a year. Care will be taken to perform these reviews in an environment and manner that promotes contributions from the staff and makes them part of the effort of defining the procedures and proper levels of security.

Proprietary information will be clearly identified. The FH Security Policy & Procedure document will emphasize to staff the importance of security in general. Staff are required to make use of this mechanism to maintain a sufficient level of awareness of security issues.
Supervisors will consider security procedure compliance when completing staff performance evaluations. Security issues will be addressed with departing staff during exit interviews performed by HR.

ASSURANCE

Defining and implementing appropriate security levels requires a continual process of confirming that both the defined policies and procedures are adequate for the ongoing work of FH, and that those policies and procedures are being properly communicated to and carried out by the staff and users. FH provides such assurances through a number of organizational and operational facets.

Chief Security Officer

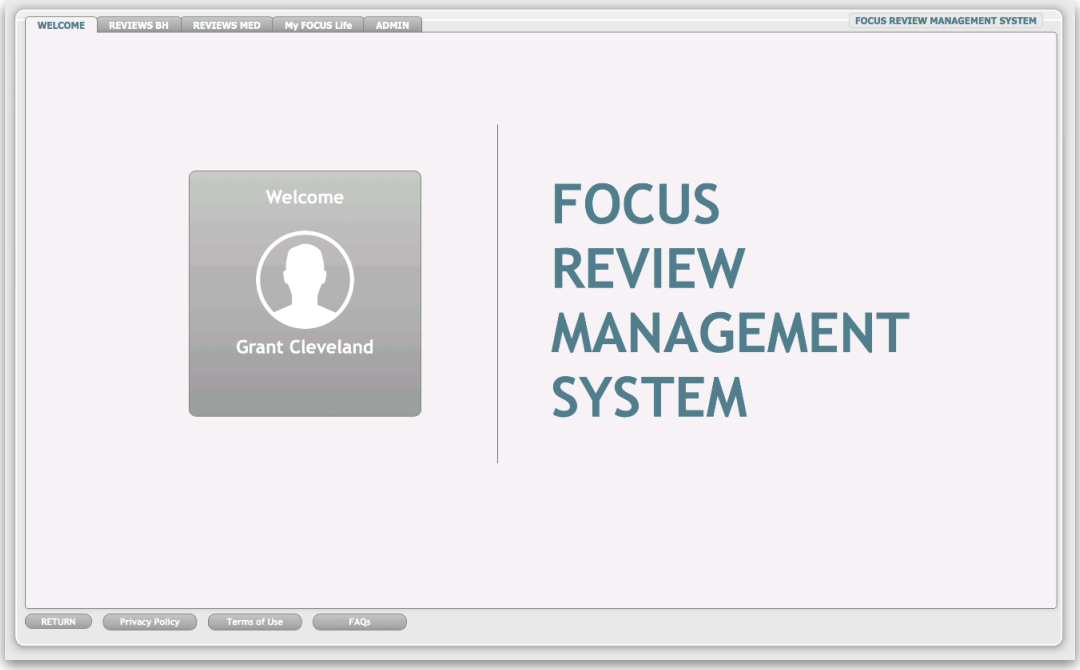
The FH Chief Security Officer helps to set guidelines and insure the integrity of the FH computer and network environment. The FH CSO will actively track and respond to security vulnerabilities and incidents. The CSO shall regularly send security reminders to FH staff and peer reviewers as well.

Staff Responsibilities

All FH staff members are responsible for executing policies and procedures in their function. It is the FH Chief Security Officer's responsibility to see that the detailed procedures section is maintained and followed in the daily activities of the staff in that area. The CSO shall respond to requests for information from staff on specific procedures and interpretation of security policies. It is the responsibility of each staff member to follow the procedures defined for an area in which he or she is engaged. It is also their responsibility to understand the underlying policies that drive those detailed procedures, so that the individual is able to make rational decisions in certain situations not specifically covered by the detailed procedures. However, in the latter case, a further responsibility exists to report the situation and have procedures clarified for future reference by other staff. Each staff member is expected to report any known or suspected violations of security procedures, or any exposure of known sensitive material to unauthorized personnel. This report should be made immediately to the FH Chief Security Officer.
FH Staff and FH peer reviewers are required to read and sign the FH Security Policy & Procedure at least annually.

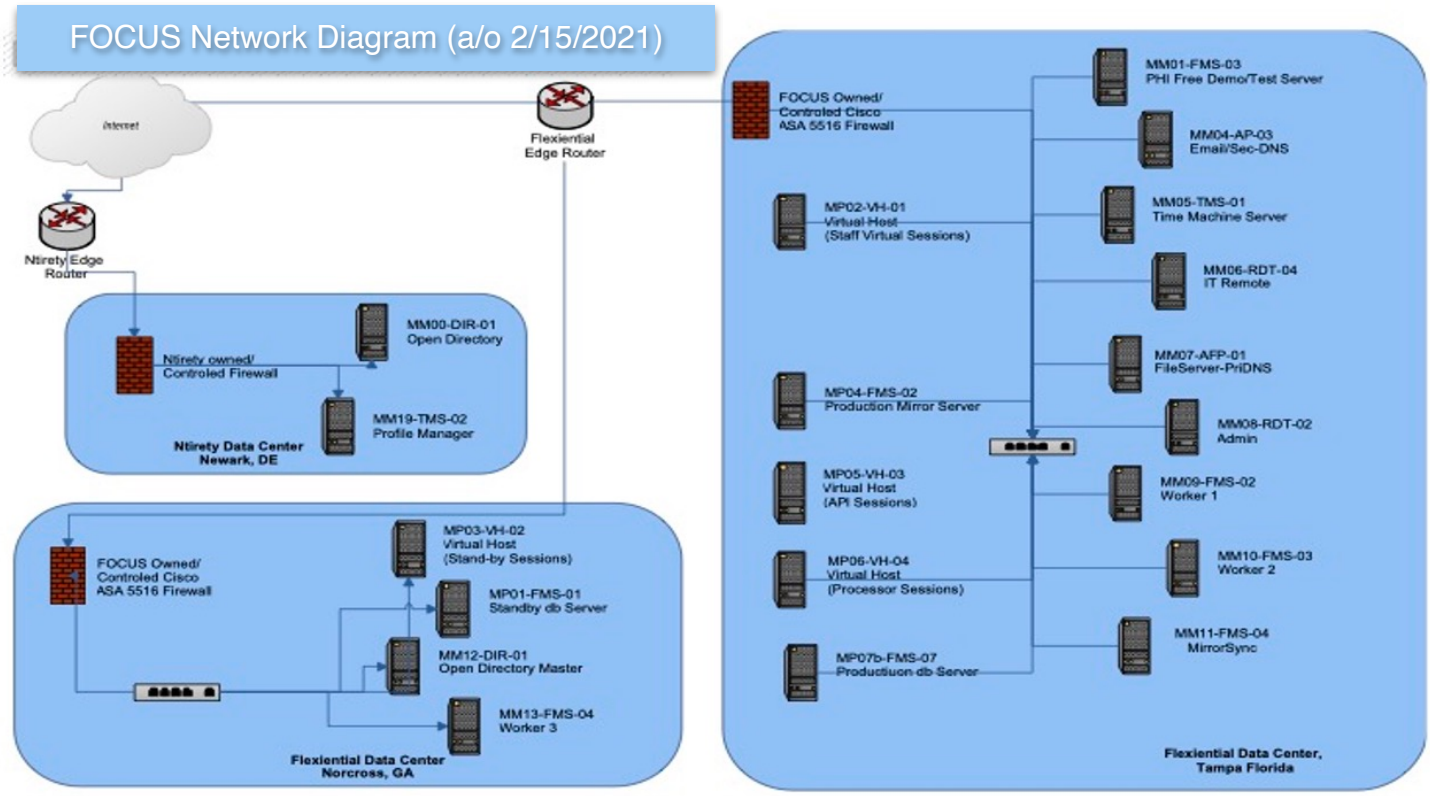
FH Review Management System

The FH Review Management System (RMS) is an internally developed, centralized system that collects, maintains and analyzes information necessary for organizational management that provides for data integrity, includes a plan for storage, maintenance and destruction, includes a plan for interoperability between internal systems and external entity information systems URAC C-13, including sensitive information Personal Health Information (PHI) and Personally Identifiable Information (PII). The RMS provides all FH stakeholders with a User Interface (UI) that provides only the necessary functions required to each user based on their privilege set so as to limit exposure of data. All data is stored and hosted from a central server located in a primary data center and a secondary (failover) datacenter. The FH RMS is a relational database that is securely accessed by either a web browser or an executable application installed on virtual sessions accessible by FH Employees. Secure internet connections provide high performance access to FH resources. Internet access is provided to authorized personnel through a device known as a security appliance (sophisticated firewall) which is configured with a number of packet filters and other "firewall" mechanisms in order to prevent certain types of attacks from entering the FH intranet housed within the datacenter.



FH Network Diagram

The illustration below shows the network diagram and hardware implemented within the primary datacenter which is designed to fulfill the business needs of the company. FH operates on two independent trunks (each provided by a different vendor) of fiber-optic cabling to the internet. These trunks to the internet provide access to the FH Review Management System by end users including client-company managers and care managers, FH staff members and FH peer reviewers. Between the servers and their services (including but not limited to the FH Review Management System) and the internet are firewalls designed to prevent unauthorized access to the network and servers. To provide additional security, all services are password-protected and all traffic is encrypted with 128-bit security or greater. Only FH equipment is allowed to be connected to the FH network in the FH server facility. This includes personal laptops or other personal devices. The Chief Security Officer is responsible for validating data input/output.



Violations and Recommended Disciplinary Sanctions
Also see *'Formal Sanctions Policy'* page 27.

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, and/or authorized designee. • Discarding PHI improperly (written) • Attempting to or succeeding to modifying, altering, deleting, or disabling anti-virus/anti-malware software. • Leaving PHI unprotected
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

FOCUS Health, Inc. will utilize the following recommendations in determining the types of disciplinary actions to take when a violation occurs:

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on Security awareness • Retraining on Information Security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand; or suspension • Retraining on Security awareness • Retraining on Information Security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Administration's discretion to report the incident to licensing boards, registration entities, and certification entities • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. When appropriate, progressive disciplinary action steps shall be followed allowing the employee to correct the behavior which caused the disciplinary action.

Exceptions: Depending on the severity of the violation, any single act may result in disciplinary action up to and including termination of employment or contract with FOCUS Health, Inc.

Table of Allowed and Prohibited Computing Devices

The following table defines categories of computing devices and acceptable use:

Device Type	Location	Role
Servers (FileMaker Server, DNS Server, Open Directory Server, Remote Session Servers)	DataCenters	Allowed
Ancillary Processors (Computers which assist in FileMaker Automation)	DataCenters	Allowed
Desktop Computers (Client-Companies, Peer Reviewers, FOCUS Employees)	Home/Office	Allowed
Laptop Computers (Client-Companies, Peer Reviewers, FOCUS Employees)	Home/Office	Allowed
Tablets (iOS/Android) using web browser or app via VPN	Prohibited*	Prohibited*
Mobile Phones (iOS/Android) using web browser or app via VPN	Prohibited*	Prohibited*

* Prohibited is defined as:

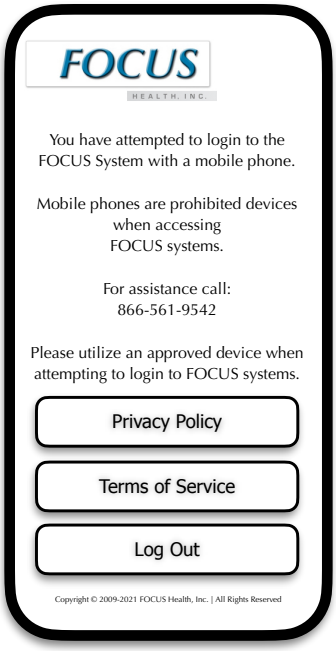
1) The FOCUS Review Management System auto-senses the device type and prevents logging in to access the system if the device is iOS or Android based; and

2) The FOCUS Security Policy clearly states that tablets and mobile phones (iOS/Android Devices) are prohibited devices; and

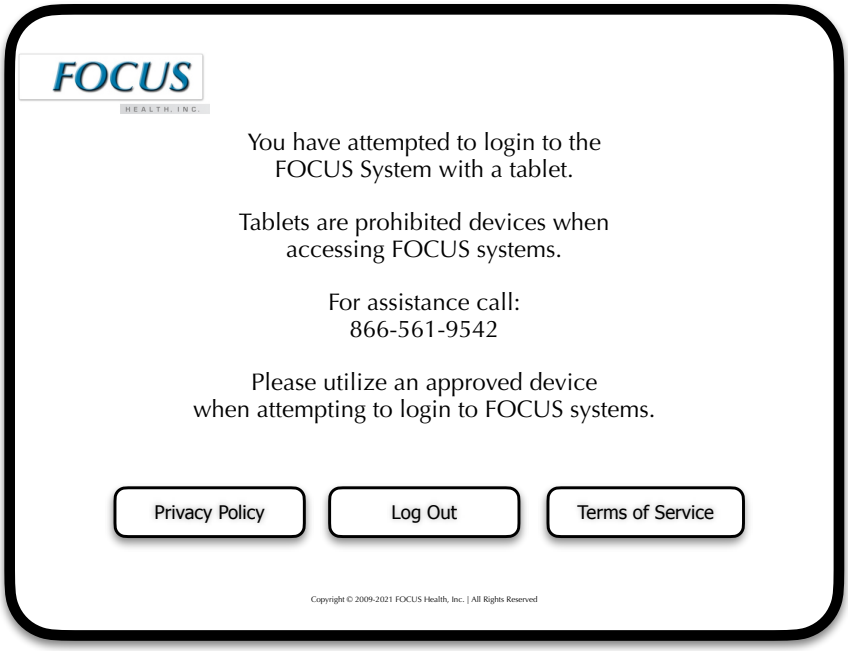
3) FOCUS Employees and Peer Reviewers must read and attest to all training materials and Policies & procedures prior to accessing the FOCUS RMS system and annually thereafter.

4) The below screen is displayed in the event a user attempts to login with a prohibited device:

Mobile Phone



Tablet



Index of Referenced Documents

This document references the following separate instruments which provide additional details:

Policies & Procedures	Supporting Documents
Access Control Policy	Risk Assessments
Clean Desk Policy	Disaster Recovery Business Continuity Plan
Code of Conduct	Business Continuity Plan Test
Complete Disaster Recovery Plan	OWASP T10 Security Policy
Confidentiality of Personal Health Information (PHI)	Disaster Recovery Business Continuity Plan
Consumer Communication	
Employee Onboarding & Offboarding Policy	
HIPAA Policy	
Mobile Device Policy	
Risk Assessment Policy	
Security Policy (Simplified)	
Software Development Life Cycle	
Staff Training Agenda	
Storage and Destruction Policy	
Systems Interoperability Policy	
Telecommuter Confidentiality Policy	

01 Information Protection Program

FOCUS implements information system(s) (electronic and paper) to collect, maintain and analyze information necessary for organizational management that:URAC C-13 (No Weight)

(a) Provides for data integrity; (Mandatory)
(b) Includes a plan for storage, maintenance and destruction; and (2)
(c) Includes a plan for interoperability: (No Weight)
    (i) Between internal information systems; and (Leading Indicator)
    (ii) With external entity information systems. (Leading Indicator)

POLICY: These URAC standards are implemented within the **FOCUS Information Protection Program**[(a)(c)]; the **FOCUS Security Policy and Procedure**[(a)(c)] and the **FOCUS Storage and Destruction Policy and Procedure**[(b)]. Measurement of success is based on the creation, maintenance, and accurate execution of these FOCUS Policies and procedures, monitoring data entry personnel for accuracy; cross-checking databases for consistency; using unique identifiers for data; prevention of and checking for duplicate entries; required creation and assessments of generated reports, logs, plans or other evidence as documented in committee meetings. Ongoing quality assurance monitoring mechanisms include annual review of the programs, policies and procedures, and ongoing monitoring of reports and logs with quarterly committee meetings. All annual and monitoring activities are to be entered into the FOCUS Calendar.

PROCEDURES:

— The FOCUS CSO is to direct and manage the continued optimization of the RMS to ensure that security and continued customization and functionality of the RMS meets or exceeds company requirements, client-company requirements, regulatory requirements and FOCUS business needs
— The FOCUS CSO and IT team members are to provide for data integrity through implementing security controls, data integrity checks and system redundancy
— The FOCUS CSO and IT team members have developed a plan for storage, maintenance and destruction (see FOCUS policy entitled 'Storage and Destruction' for detailed procedures).
— The FOCUS CSO and IT team members have developed a plan for interoperability (see FOCUS policy entitled 'Systems Interoperability Policy').

MONITORING:

— The FOCUS CSO is responsible to hold quarterly meetings to review reports and logs, discuss current topics related to this standard,

EVIDENCE:

— Documentation of all meetings between FOCUS and the client-company.
— Documentation of ICD plans.
— Documentation of test results and action items to modify the system so that testing is confirmed.
— Documentation of results after the go-live date to ensure success of the project.
— Documentation of subsequent meetings, modifications, alterations, testing and supplemental go-live results.

RESPONSIBLE PARTY:

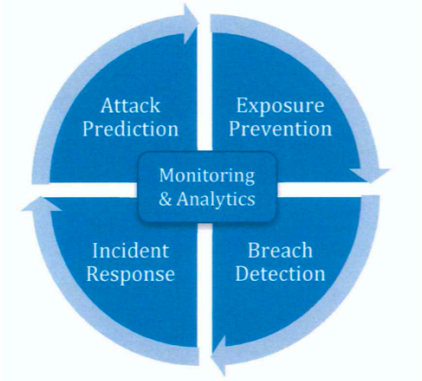
• FOCUS Chief Security Officer

POLICY: FOCUS Has a formal information protection program based on an accepted industry framework that is reviewed and updated as needed.[0101.00a1Organizational.123] The **FOCUS Information Protection Program**, based on FOCUS policies and procedures, provides our Organizational Mission Statement, Program Purpose, Program Goals, Scope, Authority and Accountability, Definitions and Standards to be met. Measurement of success for this FOCUS Program is based on the creation, evaluation, modifications and appointed attestions (approval) of FOCUS Policies and Procedures no less than annually. Ongoing quality assurance monitoring mechanisms include semi-annual review, modifications, distribution and training of stakeholder applicable Policies and Procedures. The FOCUS Information Protection Program shall be reviewed and if necessary, updated no less than annually. All annual and monitoring activities shall be entered into the FOCUS Calendar.

Examine policies and/or standards related to the information security management program (ISMP) and determine if the ISMP is documented that addresses the overall security program of the organization. Management support for the ISMP is demonstrated through signed acceptance or approval by management. The ISMP considers all the HITRUST Control Objectives and documents any excluded control domains and the reasons for their exclusion. The ISMP is updated at least annually or when there are significant changes in the environment.

ORGANIZATIONAL MISSION STATEMENT:
FOCUS Health is dedicated to providing the highest quality physician review services to help ensure that patients receive evidence based, medically necessary health care in the least restrictive setting.

PROGRAM PURPOSE:
The FOCUS Health Chief Security Officer is committed to engaging and working to identify, develop, seek approval for, and promote a comprehensive information security and risk management program. The program will focus on attack prediction exposure prevention, breach detection and incident response through continuous monitoring. It is the mission of the CSO to utilize user education, Governance, Risk management and Compliance (GRC) to meet the needs of FOCUS health and supports its organizational mission, while protecting FOCUS Health assets against unauthorized use, disclosure, modification, damage and loss.



PROGRAM GOALS:

Goal 1: Identify, approve and promote a best practice IT security standard.

The CSO, in partnership with all appropriate stakeholders and committees, will guide FOCUS Health in the selection of an appropriate information security standard that best serves the mission of the company.

Key Benefits
— Provide a clear information security baseline for all stakeholders.
— Serve as a catalyst for implementing secure business processes.
— Provide a security model for policy development.

Goal 2: Develop, approve and promote a comprehensive set of IT security policies.

The CSO, in partnership with all appropriate stakeholders and committees, will guide FOCUS Health in the development of a comprehensive set of information security policies. Policies will be based on the information security standard selected in Goal 1, will follow information security best practices, and will be tailored to best support the mission and risks of FOCUS Health.

Key Benefits
— Consistent information security controls across all stakeholders and processes.

— Topic specific and focused baseline for implementing information security controls.
— Foundation for implementing and measuring compliance.
— Clear security role responsibility and accountability.
— Consistent prevention and remediation processes.

Goal 3: Implement a formal risk and contingency management program.

The CSO will drive the development and implementation of an IT centric business impact analysis and risk assessment, which will provide FOCUS Health necessary information and tools to identify its mission essential business functions, understand their relationships, and quantify the risk associated with their disruption. Subsequently, a business continuity and disaster recovery plan will be established to provide continuing of mission essential functions that are dependent upon IT systems. A schedule for periodic testing of these plans will be established.

Key Benefits
— Continuous improvement through a regular risk and maturity assessment testing.
— Recovery of IT systems and services according to critical business units' needs.
— Identification of FOCUS Health's mission critical functions related to IT systems.
— Improved visibility over business function dependencies.
— A risk based approach to information security.

Goal 4: Inventory and classify sensitive systems and data.

The CSO will initiate a companywide inventory process to identify and classify sensitive systems and data. Sensitive systems dan d data will be protected in accordance with the policies set forth by the Company under Goal 2 and following guidance from appropriate Stakeholders. Sensitive data no longer needed for business or archival purposes will be managed based on FOCUS Health retention policies.

Key Benefits
— Reduced risk of exposure of sensitive systems and data sets.
— Consistent classification, management, and protection of sensitive data.
— Improved compliance for HIPAA, HITRUST, URAC and other requirements.
— Holistic view and inventory of sensitive systems and data.

Goal 5: Establish a broad information security educational and training program.

The CSO shall establish and maintain a broad ongoing information security awareness program in support of Goal 2. The information security awareness program shall be well integrated into FOCUS Health's Review Management System, on-boarding and off-boarding workflow, include relevant education material and training tailored to Stakeholders, and provide measurable results of effectiveness. The CSO shall provide business continuity and disaster recovery training to FOCUS employees no less than annually.

Key Benefits
— Improved employee recognition of and response to potential and real security concerns.
— Improved awareness of security threats and their impact on information assets.
— Reduced number of incidents from social engineering and other attacks.

Goal 6: Align Governance and IT to support information security and risk reduction.

FOCUS Health will align and strengthen relevant current governance committees, and establish new governance committees as needed to infuse and drive information security across all aspects of the business. The CSO and CSO will assess IT requirements and align processes to enhance technical and management IT security controls, implement new controls where needed, and monitor the effectiveness of the controls.

Key Benefits
— Improved information flow among all Stakeholders.
— Improved awareness of perceived risk, and risk appetite by the CSO.
— Ability to make more informed risk based decisions across the Company.
— Support and implement the 'security is a shared responsibility' model.

Goal 7: Establish a process for regular progress reporting.

The CSO will establish a vehicle and schedule for reporting on the process of this information security strategic plan between various Stakeholders, and senior leadership.

Key Benefits

— Visibility over governance, risk and compliance status and progress.
— Ability to make informed risk based decisions.

SCOPE:

In formulating and implementing the Plan, we will (1) identify reasonably foreseeable internal and external risks to the security, confidentiality, and/or integrity of any electronic, paper or other records containing personal information; (2) assess the likelihood and potential damage of these threats, taking into consideration the sensitivity of the personal information; (3) evaluate the sufficiency of existing policies, procedures, customer information systems, and other safeguards in place to control risks; (4) design and implement a plan that puts safeguards in place to minimize those risks, consistent with the requirements of FOCUS Health's accrediting and certifying bodies, and (5) regularly monitor the effectiveness of those safeguards.

AUTHORITY AND ACCOUNTABILITY:

The FOCUS Health Chief Security Officer is the appointed authority whose role is to provide oversight and direction regarding information systems security and privacy assurance Company-wide. In collaboration with the Chief Security Officer (CSO), the CSO's specific oversight responsibilities include the following:

- Oversee the development, implementation, and maintenance of a Company-wide strategic information systems security plan.
- Oversee the development, implementation, and enforcement of Company-wide information systems security policy and related recommended guidelines, operating procedures, and technical standards.
- Oversee the process of handling requested policy exceptions
- Advise senior administrators of FOCUS Health on related risk issues and recommend appropriate actions in support of FOCUS' larger risk management programs.

DEFINITIONS OF STANDARDS TO BE MET:

FOCUS Health is required to meet or exceed standards as put forth by Federal and State regulatory requirements, as well as the HITRUST Alliance and URAC. Below are the definitions of some standards FOCUS Health must meet:

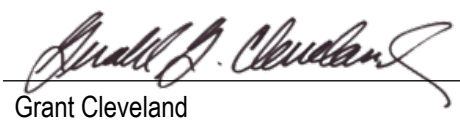
— Approved Endpoint Software such as Virus/Malware protection software, Apple MDM Software (for remote management of workstations) and approved programs (applications available to end-users, such as Microsoft Office).

— Data protection safeguards of physical controls, approved data centers, ID badges to enter data centers, firewall hardware to protect data, security patches (software updates), data encryption, Antivirus updates, security testing, proper disposal.

— Data categorization (public use, internal use, sensitive use, highly sensitive use)

— Encryption standards (Cryptography is the practice or study of hiding information. That is, devising a way to encrypt information. Key Management is the management of cryptographic keys including dealing with the generation, change, storage, use, and replacement of keys.)

— Network firewall standards (A firewall, or 'Security Appliance' is a device that requires programming in order to configure the device to maximize security).



Grant Cleveland
President, Chief Security Officer and Chief Security Officer

PROCEDURES:

- Accessing the Review Management System, FOCUS Management shall hold documented meetings no less than annually to review, update and optimize the FOCUS Information Protection Program and its elements including (but not limited to):

  — Review and/or modify the Information Protection Program and all subordinative elements
  — Distribute and provide training to all applicable stakeholders with their respective Policies and Procedures

- The FOCUS CSO shall (no less than annually) deliver training to all FOCUS employees and contracted Peer Reviewers to ensure users are aware of their responsibilities during a disaster.

MONITORING:

- FOCUS Management shall enter into, monitor and ensure compliance with all FH calendar entries to fulfill requirements as set forth by the FOCUS Information Protection Program.

EVIDENCE:

- Calendar entries; documentation of original and updated versions of the Information Protection Program; documentation of original and updated version of Policies and Procedures; documentation of training logs and attestations of all trainees within the FOCUS RMS.

PRIMARY RESPONSIBLE PARTY:

- Chief Security Officer

REQUIRED PARTICIPANTS:

- FOCUS Chief Medical Officer, Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Security Officer, Chief Operating Officer.

ENFORCEMENT:

- Meetings shall be held with all required personnel prior to completion deadline established by the FOCUS CSO.
- Ratification of all applicable FOCUS policies & procedures must be completed on or prior to the deadline established by the FOCUS CSO.
- In the event the FOCUS CSO is for any reason unavailable to complete duties, the FOCUS CEO shall fulfill the primary responsibilities of the FOCUS CSO.

SUPPORTING POLICIES & PROCEDURES:

- Staff Training Agenda (RMS » ADMIN » ORGANIZATION » P&Ps » STAFF TRAINING AGENDA)

POLICY:

FOCUS shall ensure that an information protection program is formally documented and actively monitored, reviewed and updated to ensure program objectives continue to be met.0102.00a2Organizational.123 This is achieved by the **FOCUS Information Protection Program** which stipulates that the FOCUS CEO and FOCUS CSO must annually review the content of the FOCUS Information Protection Program, and semi-annually the CSO must re-review the FOCUS Information Protection Program. Measurement of success for this FOCUS policy is based on evidence collected by documented annual and semi-annual review and re-review of the FOCUS Information Protection Program. Ongoing quality assurance monitoring mechanisms include entries into the FOCUS Annual Calendar, review of meeting minutes and oversight by the FOCUS CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the information security management program (ISMP) and determine if a program has been established, implemented, operational, monitored, reviewed, and maintained. The ISMP is formally documented, protected, controlled, and retained according to federal, state and organizational requirements. The ISMP also incorporates a Plan, Do, Check, ACT (PDCA) cycle for continuous improvement in the ISMP, particularly as information is obtained that could improve the ISMP, or indicates any shortcomings of the ISMP.

PROCEDURES:

- The FOCUS Administrative Team reviews this policy and enters it into the company calendar to ensure annual review; and
- The FOCUS CSO enters it into the company calendar to ensure semi-annual review; and
- Documented, formal Meetings will be held by all required participants (see below) to review all policies & procedures applicable to the information protection program; and
- The FOCUS CSO schedules virtual (Zoom) meetings and share the P&P meeting and review screens provided by the FOCUS RMS Administration screen located at ADMIN » ORGANIZATION » P&Ps » SECURITY POLICY and will select the next, unapproved version of the policy for review; and
- The FOCUS CSO shares and document the meeting minutes located at ADMIN » ORGANIZATION » MEETINGS » POLICY AND PROCEDURE REVIEWS and will document the meeting minutes; and
- The FOCUS Administrative Team reviews this policy annually and make it effective at least annually; and
- The FOCUS CSO schedules Policy & Procedure Review Meetings with the FOCUS Administrative Team. Upon completion of modifications and with full agreement, the CMO/CEO, CIO/CSO, CFO and COO authorizes all policies and procedures by signature attestation that apply to and support the Information Protection Program; and
- The CSO reviews the policy on a semi-annual basis and if any modifications are proposed, the FOCUS Administrative Team reviews recommended changes to any applicable policies and make these policies effective upon ratification at that time.

MONITORING:

- Company calendar entries; CSO semi-annual review; Administrative Team annual review.

EVIDENCE:

- Company calendar entries; meeting minutes; ratified version history of policies that are attributable to the FOCUS Information Protection Program.

PRIMARY RESPONSIBLE PARTY:

- Chief Security Officer.

REQUIRED PARTICIPANTS:

- FOCUS Chief Medical Officer, Chief Executive Officer, Chief Financial Officer, Chief Information Officer, Chief Security Officer, Chief Operating Officer.

ENFORCEMENT:

- Meetings are held with all required personnel prior to completion deadline established by the FOCUS CSO.
- Ratification of all applicable FOCUS policies & procedures are completed within the FOCUS RMS on or prior to the deadline established by the FOCUS CSO.

SUPPORTING POLICIES & PROCEDURES:

- Location of Policies & Procedures: RMS » ADMIN » ORGANIZATION » P&Ps » (Select Policy & Procedure) » (Select Version).
- Each FOCUS Security Policy & Procedure listed within this document will specify any separate independent policy and procedure documents, as applicable.

POLICY: FOCUS shall ensure that user security roles and responsibilities are clearly defined and communicated.0104.02a1Organizational.12 This is implemented as a policy and procedure within the **FOCUS Security Policy.** Measurement of success for this FOCUS policy is based on evidence collected by clearly written roles and responsibilities within each **FOCUS Job Description,** as delivered per the **Employee On-boarding & Off-boarding Policy** and the **FOCUS Staff Training Agenda.** Ongoing quality assurance monitoring mechanisms include annual review and CEO authorized job descriptions and attested (signed) evidence of each FOCUS staff member reading, understanding and accepting of their respective job description annually. Any interim modification of job descriptions must be presented to affected FOCUS staff members for interim attestation by the staff member. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user roles and responsibilities and determine whether they include: (i) implementing and acting in accordance with the organization's information security policies; (ii) protecting assets from unauthorized access, disclosure, modification, destruction or interference; (iii) executing particular security processes or activities; (iv) ensuring responsibility is assigned to the individual for actions taken; (v) reporting security events or potential events or other security risks to the organization; and, (vi) security roles and responsibilities are defined and clearly communicated to users and job-candidates during the pre-employment process.

PROCEDURES:

Accessing the Review Management System, FOCUS Management ensures that:

— Each job description is to have clearly written security roles and responsibilities; and
— Each FH Staff Member has annual training which includes review of his/her job description; and
— Each FH Staff Member has 24/7 access to the FOCUS CSO in the event there are security questions regarding roles and responsibilities.

MONITORING:

- FOCUS Management monitors to ensure compliance with applicable FH calendar entries; ensures that during each annual job description review meeting that any modifications are reflected in the latest version of the Job Description; and ensures that all new hires are processed per requirements stated in the Employee Onboarding & Off-boarding Policy and the FH Staff Training Agenda, including all security elements.

EVIDENCE:

- Calendar entries
- Documentation of FOCUS Management meeting minutes pertaining to policy and/or job description modifications
- Version history of all updated FOCUS Job Descriptions
- Version history of all updated Policies and Procedures
- Documentation of training logs and attestations of all trainees within the FOCUS RMS and clearly written roles and responsibilities within job descriptions including all security roles and responsibilities.

POLICY: FOCUS shall have an information security workforce improvement program.[0107.02d1Organizational.1] This program is documented within the FOCUS Information Protection Program and applicable to all FOCUS staff members which receive training on instructions specified within the applicable **FOCUS Job Description, FOCUS Staff Training Agenda** and **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence of the delivery of initial and annual staff member training with attestations from each staff member that they have read and understand all training materials. Ongoing quality assurance monitoring mechanisms include interim training events as needed (with updated attestations) when policies or training materials are added, modified or deleted. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
Utilizing the FOCUS RMS training module, the FOCUS CSO ensures that:
— The Training Agenda is updated to include curriculum that meets all topics required to ensure compliance with Federal, State, URAC, and HITRUST standards and requirements; and
— Ensuring that role-based training and measurements are defined within the 'Staff Training Agenda Policy; and
— Each new hire is to be provided documented, initial training (Job Description, Staff Training Agenda Items and Security Policy); and
— Each new hire is to attest to receiving and understanding all training materials; and
— Each staff member is to be provided documented, annual training (Job Description, Staff Training Agenda Items and Security Policy); and
— Each staff member is to attest to receiving and understanding all training materials; and
— Ongoing quality assurance monitoring mechanisms include interim training events as needed; and
— Interim training events are to be documented with end-user attestations that information is received and understood; and
— Each training event (either for new hires or team training events) are to be logged into the FH Calendar within the RMS.

MONITORING:
- The FOCUS CSO monitors and ensures compliance with applicable FH calendar entries; and ensures that all new hires are trained on security matters documented within the FOCUS Job Description and the FH Staff Training Agenda; initiates interim training events in the event modifications to FOCUS Policies and Procedures or Training Agendas are made.

EVIDENCE:
- Calendar entries; documentation of training logs; attestations from all staff members upon receipt and understanding of Job Descriptions and FOCUS Security Policy training.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

SUPPORTING POLICIES AND PROCEDURES:
- Staff Training Agenda (RMS » ADMIN » ORGANIZATION » P&Ps » STAFF TRAINING AGENDA)

POLICY: FOCUS shall author plans for security testing, training and monitoring activities are developed, implemented, maintained and reviewed for consistency with the risk management strategy and response priorities.0108.02d1Organizational.23 Processes to achieve a comprehensive approach to security are documented in the **FOCUS Security Policy & Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by documented annual **Penetration Test Report**, documented initial and annual training for each FOCUS staff member and Peer Reviewer as well as annual **FOCUS Risk Assessments** and **FOCUS Disaster Recovery Test Reports.** Ongoing quality assurance monitoring mechanisms include periodic review of **RMS Access Logs** to examine authorized access, unauthorized access and administrative activity; re-evaluation of annual training events, annual FOCUS Risk Assessments and annual FOCUS Disaster Recovery Tests. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to management responsibilities and determine whether the organization ensures plans for security testing, training and monitoring activities are developed, maintained, and executed in a timely manner. The organization reviews testing, training and monitoring plans for consistency with the organizational risk management strategy and organization-wide priorities for risk response actions.

PROCEDURES:

— CSO identifies, contracts with and outsources to qualified firm to conduct penetration test and provide FOCUS with a detailed penetration testing and account login testing report annually.

— Per the FOCUS Onboarding Policy & Procedure as well as the FOCUS Staff Training Agenda, security and disaster recovery process training is provided to all new contracted Peer Reviewers and Employees as well as annually to current Peer Reviewers and Employees. Attestations by recipients shall be acquired confirming that they have received and understand training materials:
  - Security training administered with attestations by each attendee no less than annually; and
  - Monitoring includes:
    - CSO review of incoming reports of perceived or actual security risks from the on-screen form within the FOCUS RMS; and
    - CSO review of incoming reports of perceived or actual security risks from the anonymouos security web form; and
    - CSO review of Anti-Virus/Anti-Malware reports; and
    - CSO review of RMS logs that report successful and unsuccessful attempts to login to the FOCUS RMS.

— CSO to review and update FOCUS Risk Assessment documentation no less than annually.

— CSO to conduct Incident Response Plan Tests with participation of key security related personnel no less than annually.

— CSO to schedule and ensure that FOCUS IT staff members participate in a Disaster Recovery Test and generate a complete report no less than annually.

MONITORING:

- The FOCUS CSO documents steps taken to periodically review and evaluate security policies and procedures, penetration test reports, risk assessments, RMS Access Logs, the FOCUS Calendar and the FOCUS Training Agenda.

EVIDENCE:

- Calendar entries; documentation of training logs; scheduled training events; training participant attestations for security training; training participant attestations for disaster recovery processes; Annual penetration test report; FOCUS Risk Assessment; FOCUS Disaster Recovery Test Reports; RMS Access logs.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

SUPPORTING POLICIES AND PROCEDURES:

Location of policies: RMS » ADMIN » ORGANIZATION » P&Ps » [Policy]

- FOCUS Onboarding & Offboarding Policy
- Incident Response Plan

SUPPORTING DOCUMENTS:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » Supporting Documents » [Document]

- Incident Response Plan Test Form
- Disaster Recovery / Business Continuity Plan

POLICY: FOCUS Management shall ensure that users are briefed on their security role(s)/responsibilities, conform with the terms and conditions of employment prior to obtaining access to FOCUS information systems; are provided with guidelines regarding the security expectations of their roles; are motivated to comply with security policies; and continue to have the appropriate skills and qualifications for their role(s).0109.02d1Organizational.4 This is achieved by initial and annual training as specified in the **FOCUS Onboarding Policy & Procedure** **and** **FOCUS Staff Training Agenda Policy & Procedure** with attestations to reading and understanding of all materials. Measurement of success for this FOCUS policy is based on evidence collected by initial and annual **background checks** and research documentation on each FOCUS Staff Member candidate; initial and annual attestation to all training materials with emphasis that the user understands all materials; a comprehensive training agenda and attestations to receiving initial training for each new hire; evidence of continued annual training and assurance that each FOCUS Staff Member maintains skills required to fulfill their duties. Ongoing quality assurance monitoring mechanisms includes annual evaluation of onboarding requirements; annual management evaluation of training materials to ensure compliance a nd thoroughness; and assurance that FOCUS Staff Members are motivated to comply with all requirements. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to management responsibilities and determine whether management responsibilities includes ensuring that employees, contractors and third-party users: (i) are properly briefed on their information security roles and responsibilities prior to being granted access to covered information or information systems; (ii) are provided with guidelines to state security expectations of their role within the organization; (iii) are motivated and comply with the security policies of the organization; (iv) achieve a level of awareness on security relevant to their roles and responsibilities within the organization; (v) conform to the terms and conditions of employment, which includes the organization's information security policy and appropriate methods of working; and, (vi) continue to have the appropriate skills and qualifications.

PROCEDURES:

Utilizing the Review Management System's training and documentation deployment module:

— Per the FOCUS Onboarding Policy & Procedure as well as the FOCUS Staff Training Agenda, background checks must be completed and approved by management, followed by security training for all new contracted Peer Reviewers and Employees prior to accessing FOCUS Information Systems, as well as annually to current Peer Reviewers and Employees. Attestations by recipients are to be acquired confirming that they have received and understand training materials.

— The CSO will ensure that the FOCUS Review Management System has posted to a splash screen at startup to display information regarding the importance of following the security policy and all possible company and/or end user sanctions in the event of inappropriate activities.

— Senior Management to annually review Job Descriptions to ensure that guidelines regarding required continued appropriate skills and qualifications as well as security expectations are present.

MONITORING:

- FOCUS Management will schedule and periodically review the inventory of background checks on Employees and Peer Reviewers, as well as training records to ensure compliance with the FOCUS Onboarding Policy & Procedure; ensure that end-users continue to be presented with on-screen policy reminders and sanctions; and review of Job Descriptions to ensure they are up-to-date.

EVIDENCE:

- Calendar entries; Job Description Updates; Screenshots of policy/sanction reminders; Training logs; Background Checks.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

SUPPORTING POLICIES AND PROCEDURES:

Location of policies: RMS » ADMIN » ORGANIZATION » P&Ps » [Policy]

- FOCUS Onboarding & Offboarding Policy
- Staff Training Agenda

POLICY:
If the senior-level information security official is employed by FOCUS, one of its affiliates, or a third party service, FOCUS shall retain responsibility for its cybersecurity program, designates a senior member of FOCUS responsible for direction and oversight, and requires the third party service to maintain an appropriate cybersecurity program of its own.01110.05a1Organizational.5 This is achieved by the **FOCUS Cybersecurity Program** which dictates the FOCUS CSO is responsible for the FOCUS Cybersecurity program. Measurement of success for this FOCUS policy is based on evidence collected by attestation from the FOCUS CSO regarding this assignment, as well as incorporation of this responsibility within the **FOCUS CSO job description**. Further, all policies and procedures regarding cybersecurity shall be stipulated in the **FOCUS Security Policy and Procedure**. Ongoing quality assurance monitoring mechanisms include annual review of the FOCUS CSO Job Description by the CEO as well as the FOCUS Cybersecurity Program and FOCUS Security Policy and Procedure. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to management's commitment to information security to determine if a senior-level information security official is employed by the organization, one of its affiliates, or a third-party service, the organization (i) retains responsibility for its cybersecurity program in compliance with applicable regulatory requirements; (ii) designates a senior member of the organizations personnel responsible for direction and oversight of the third-party service provider; and, (iii) requires the third-party service to maintain a cybersecurity program that protects the organization and complies with applicable regulatory requirements.

It is the policy of FH to maintain a technical and contractual relationship with a third party remote colocation hosting service for FH primary data center and FH secondary data center to host FH Servers. In the rare event the FH primary server colocation hosting site is unavailable, operations may continue upon activation of the remote hosting site. Upon activation of the FH Disaster Recovery Plan, in the event of the primary hosting site becoming non-responsive, the secondary hosting site is activated. The colocation vendor for both the primary and secondary hosting sites must:

- Notify FH of any predictable outages of service; and
- Notify the FH Chief Security Officer of any potential security incidents; and
- Provide FH with annual reports of external security assessments; and
- Provide FH with evidence of current, active security certifications.

PROCEDURES:
At the time of this policy effective date:
- The Chief Security Officer is required to be an employee of FOCUS (not a contracted person); and
- All responsibilities of the CSO are executed by the CSO without outsourcing to any 3rd party; and
- The CSO is solely responsible for the FOCUS cybersecurity program.
- This policy is to be reviewed and updated to include procedures for 3rd party services before any 3rd party service provider is contracted; and
- All 3rd party service providers must provide a cybersecurity program that is reviewed and approved by the FOCUS CSO; and
- All 3rd party service provider agreement documents must be reviewed by the FOCUS CSO prior to service provisioning to ensure that the service provider upholds all applicable HITRUST controls; and
- The FOCUS CSO is to document the review and approval of vendor agreements located within the RMS
- The FOCUS CSO is to schedule a review of this policy no less than annually; and
- The FOCUS CSO schedules the review into the company calendar to ensure annual review.

MONITORING:
- Meeting minutes are required to include review of this policy and document any changes in status.

EVIDENCE:
- Meeting minutes

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

SUPPORTING DOCUMENTS:
Location of documents: ADMIN » VENDORS » (Select Vendor) » DOCUMENTS.
- Primary Data Center in Tampa: Flexential
- Secondary Data Center in Atlanta: Flexential

POLICY: FOCUS shall ensure that the company information security objectives, approach, scope, importance, goals and principles for the FOCUS security program are formally identified, communicated throughout FOCUS to users in a form that is relevant, accessible and understandable to the intended reader, and supported by a controls framework that considers legislative, regulatory, contractual requirements and other policy-related requirements.0113.04a1Organizational.123 This is achieved by development and FOCUS management authorization of this **FOCUS Information Protection Program**; provided to FOCUS staff members through initial and annual training events in a non-technical 'layman's terms' version of the Program as required in the **FOCUS Onboarding Policy & Procedure** and the **FOCUS Staff Training Agenda,** which includes signature attestation upon initial hire and annually thereafter**.** Measurement of success for these FOCUS policies is based on evidence of annual review and approval of all FOCUS Programs and Policies to ensure that materials are understandable and include all legislative, regulatory and contractual requirements; and documentation in FOCUS personnel files where a staff member excels or fails to fulfill information security protocols. Ongoing quality assurance monitoring mechanisms includes a semi-annual review of all personnel files to ensure compliance with all FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

Information Security Objectives

— Insure the security and confidentiality of FOCUS' corporate and client-company information; and
— Protect against any anticipated threats or hazards to the security and/or integrity of FOCUS' corporate and client-company information; and
— Protect against unauthorized access to or use of FOCUS' corporate and client-company information that could result in substantial harm or inconvenience to FOCUS or any client-company and their members.

Information Security Approach

Modern network security requires a layered defense approach that factors in people, processes and technology. Together, such tactics—including creating a strong culture of security, conducting threat research, prioritizing assets, and deploying modern network controls—will enhance visibility and shorten threat response times, resulting in minimizing the impact of cyberattacks.

— PEOPLE: Education for stakeholders including strong passwords, avoiding suspicious emails, maintaining modern software and reporting of unusual behavior on computers.
— PROCESSES: Proactive prevention and quick response in the event of a cybersecurity incident; threat research and prioritization of assets and systems to maintain secure continuity of business.
— TECHNOLOGY: Implementation of tools based on their ability to be integrated and automated to create a Security Fabric that can facilitate the rapid detection and mitigation of threats.

Information Security Scope

— The protection of the confidentiality, integrity and availability of information; and
— The development, operation, and administration of the FOCUS Review Management System as a Service platform; and
— The secure operation of communication systems such as chat services, email services and file services.

Information Security Importance

— Reminding staff of security importance is achieved via a splash screen which users of the FOCUS Review Management System (all staff) shall see daily; and
— Development of 'layman's' version of the FOCUS Security Policy & Procedure for easy consumption, available 24/7/365 to all personnel; and
— Predetermined frequency of reviewing all security-associated policies, procedures, work plans, job descriptions and personnel files for completeness.
— Predetermined frequency of training and attestations to all FOCUS policies & procedures applicable to job descriptions, including all security related policies.

Information Security Goals

— For FOCUS Administrators to follow the FOCUS Security Policy & Procedure and fulfill all requirements; and
— For all stakeholders (FOCUS Administrators, staff, contract Peer Reviewers) to fulfill their obligations and duties as directed within the FOCUS Security Policy & Procedure.
— To honor and abide by the defined *Objectives*, *Approach*, *Scope*, and *Importance* of the FOCUS Security Policy & Procedure.

Information Security Principles

— Based on the industry standard 'CIA Triad' of *Confidentiality*, *Integrity* and *Availability:*
  - **Confidentiality** measures are designed to protect against unauthorized disclosure of information.
  - **Integrity** involves protection from unauthorized modifications (e.g., add, delete, or change) of data.
  - **Availability** is protecting the functionality of support systems and ensuring data is fully available at the point in time or period requirements by its users.

PROCEDURES:

— Utilizing the FOCUS Review Management System, FOCUS Administration team (CEO/CSO/COO) creates, maintains and provides 24/7/365 access to an understandable version of the FOCUS Security Program which includes Information security objectives, approach, scope, importance, goals and principles, and is supported by a controls framework that considers legislative, regulatory, contractual requirements and other policy-related requirements; and
— Accessing the company calendar in the RMS, FOCUS Administrators ensure that all required calendar entries are present and policy requirements are executed on a timely basis; and
— FOCUS Administration ensures that the layman's version of the FOCUS Security Policy & Procedure includes legislative, regulatory, contractual requirements and other policy-related requirements; and
— The FOCUS Review Management System to feature a 'splash screen' which reminds users of the importance of security and applicable sanctions.

MONITORING:

- FOCUS Administrators (CEO/CSO/COO) review all activities semi-annually which includes new hire and existing staff documentation, training, attestations, presence of the automated security reminder splash screen and to ensure that documents are on file and were provided to staff in a timely manner as stipulated in FOCUS policies; and
- Review and modernization of the layman's version of the FOCUS Security Policy & Procedure to ensure that it includes legislative, regulatory, contractual requirements and other policy-related requirements.

EVIDENCE:

- Meeting minutes showing review of calendar entries, modernization of job descriptions, compliance research, and distribution of *layman's version* of FOCUS Security Policy & Procedure; and
- A copy of the *layman's version* of the FOCUS Security Policy & Procedure; and
- A screenshot of the 'importance of security' *reminder notice*, presented each time a user logs in.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

SUPPORTING POLICIES AND PROCEDURES:

Location of policies: RMS » ADMIN » ORGANIZATION » P&Ps » [Policy]

- FOCUS Onboarding & Offboarding Policy
- Staff Training Agenda
- FOCUS Security Policy (Simplified)
- Telecommuter Policy

SUPPORTING DOCUMENTS:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » Supporting Documents » [Document]

- Disaster Recovery / Business Continuity Plan

POLICY:
The FOCUS CSO shall ensure that FOCUS security policies are regularly reviewed and updated to ensure they reflect leading practices (e.g., for systems and services development and acquisition), and communicated throughout FOCUS.[0114.04b1Organizational.1] This is achieved by annual review of all FOCUS Programs and Policies and Procedures, as well as a 'Policy and Procedure Update' tab available to all FOCUS staff members and Peer Reviewers within the FOCUS Review Management System. Measurement of success is based on evidence that all FOCUS staff members and Peer Reviewers receive, read, understand and attest to the **FOCUS Security Policy and Procedure** at least annually. Further, the FOCUS Review Management System provides 24/7/365 access to all programs, policies & procedures to all FOCUS staff members and Peer Reviewers. Ongoing quality assurance monitoring mechanisms include the FOCUS CSO reviewing personnel files quarterly; and the CSO shall notify users via email and within the FOCUS RMS with the use of 'red dot indicators' of newly modified policies for users to read, understand and attest to. The CSO shall confirm that all active personnel have received and attested to the documents; and the CSO shall fortify the **'My FOCUS Life' / 'Training' tab** with the latest security advisories within the FOCUS RMS for end-users to view. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the information security policy to determine whether the information security policy documents are reviewed at planned intervals or if significant changes occur to ensure the policies' continuing adequacy and effectiveness.

PROCEDURES:
The FOCUS CSO ensures that:
— FOCUS Management reviews, edit and ratify the FOCUS Security Policy no less than annually; and
— FOCUS Management documents the policy meeting minutes; and
— FOCUS Management ensures distribution and availability of the FOCUS Security Policy to all applicable stakeholders; and
— FOCUS Management to ensure that all applicable stakeholders receive, read and attest to the Security Policy.

- The FOCUS CSO creates a company calendar entry to coordinate a review of the FOCUS Security Policy by the FOCUS Administrative Team (CMO/CEO/CFO/CIO/CSO/COO) no less than annually; and
- The FOCUS CSO conducts research to ensure the inclusion of leading security practices to present to the FOCUS Administrative Team; and
- Documented, formal Meeting(s) are to be scheduled and held by all required participants (see below) to review all policies & procedures applicable to the information protection program; and
- The FOCUS CSO schedules virtual meetings and share the P&P meeting and review screens provided by the FOCUS RMS Administration screen located at ADMIN » ORGANIZATION » P&Ps » SECURITY POLICY and display the next, unapproved version of the policy for review; and
- The FOCUS CSO shares and documents the meeting minutes located at ADMIN » ORGANIZATION » MEETINGS » POLICY AND PROCEDURE REVIEWS and documents the meeting minutes; and
- The FOCUS Administrative Team reviews this policy annually and make it effective at least annually; and
- The FOCUS CSO schedules Security Policy & Procedure Review Meetings with the FOCUS Administrative Team. Upon completion of modifications and with full agreement, the CMO/CEO, CIO/CSO, CFO and COO authorizes all policies and procedures by signature attestation that apply to and support the Information Protection Program; and
- The CSO reviews the policy on a semi-annual basis and if any modifications are proposed, the FOCUS Administrative Team reviews recommended changes to any applicable policies and make these policies effective upon ratification at that time.

MONITORING:
- FOCUS Management enters the annual FOCUS Security Policy within the company calendar to ensure that it is held no less than annually with an automated notification alarm.

EVIDENCE:
- Calendar entries; documentation of FOCUS Management meeting minutes pertaining to the FOCUS Security Policy modifications; version history of the FOCUS Security Policy; documentation of training logs and attestations of all trainees within the FOCUS RMS.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

ENFORCEMENT:
- Meetings are held with all required personnel prior to completion deadline established by the FOCUS CSO.
- Ratification of all applicable FOCUS policies & procedures must be completed within the FOCUS RMS on or prior to the deadline established by the FOCUS CSO.

POLICY:

FOCUS shall appoint a senior-level information security official and is responsible for ensuring security processes are in place, communicated to all stakeholders, who considers and addresses organizational requirements.[0117.05a1Organizational.1] This is achieved by the **FOCUS Information Protection Program** stipulating that the FOCUS Chief Security Officer is assigned this responsibility; and that the **FOCUS Organizational Chart** reflects this responsibility to the FOCUS CSO. Measurement of success is based on annual review and approval of all FOCUS policies and procedures related to security, as well as the FOCUS Organizational Chart. Ongoing quality assurance monitoring mechanisms include semi-annual review of all policies and the FOCUS Organizational Chart by the FOCUS CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:

FOCUS Administration (CEO/CSO/COO) documents, in formal meeting minutes, that:

— A senior level information security official is appointed and responsible for ensuring security processes; and
— The appointed senior level information security official is responsible for ensuring security processes are in place, communicated to all stakeholders, who considers and addresses organizational requirements; and
— The FOCUS Organization Chart displays the appointee with the title of 'CSO' (Chief Security Officer); and
— FOCUS Administrators ensure that calendar entries are entered into the RMS to ensure that meetings are held no less than annually to ensure compliance with this policy; and
— The job descriptions of FOCUS Administrators *not appointed* as the senior level information security official instructs them to meet within 14 (fourteen) business days to appoint a new senior-level information security official in the event of his/her absence beyond 14 business days.

MONITORING:

- FOCUS Administrators must honor required meetings, per the company calendar entries, to ensure that this policy is reviewed no less than annually.

EVIDENCE:

- Calendar entries; documentation of FOCUS Administration meeting minutes pertaining to the appointment of a senior-level information security official; company organization chart clearly displaying the appointment of the security official.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

SUPPORTING DOCUMENTS:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » Supporting Documents » [Document]

- FOCUS Organizational Chart

POLICY:
FOCUS senior management shall assign an individual or group to ensure the effectiveness of the information protection program through program oversight, establish and communicate FOCUS's priorities for organizational mission, objectives, and activities, review and update of FOCUS's security plan, ensure compliance with the security plan by the workforce, and to evaluate and accept security risks on behalf of FOCUS.0118.05a1Organizational.2 This is achieved by the **FOCUS Information Protection Program** stipulating that the FOCUS Chief Security Officer is assigned this responsibility. Measurement of success for this FOCUS policy is based on confirmation program oversight through a documented quarterly analysis report detailing each aspect of this standard above. Ongoing quality assurance monitoring mechanisms include annual review and management approval of the FOCUS Information Protection Program and to assure that responsibility assignment, communication to staff members, and effectiveness of the program is fulfilled. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
FOCUS Administration (CEO/CCO/COO) documents, in formal meeting minutes demonstrating information protection program oversight, that:
— A senior level information security official is appointed and responsible for:
  • Measuring the effectiveness of the information protection program through program oversight; and
  • Establishing and communicating FOCUS's priorities for organizational mission, objectives, and activities through the RMS and training events held for all FOCUS staff members and contracted Peer Reviewers; and
  • Reviewing and updating FOCUS's security plan quarterly; and
  • Ensuring compliance with the security plan by the workforce; and
  • Evaluating and accepting security risks on behalf of FOCUS; and
— The FOCUS Organization Chart displays the appointee with the title of 'CSO' (Chief Security Officer); and
— FOCUS Administrators ensure that calendar entries are entered into the RMS to ensure that meetings are held no less than annually to ensure compliance with this policy.

MONITORING:
- The appointed senior manager honors required meetings, per the company calendar entries, to ensure that the requirements of this policy are fulfilled; and
- The results of measured effectiveness, communications to staff, modifications to the Security Plan, compliance by the workforce and attestation to accepting security risks must be presented to FOCUS Administrative staff in documented meeting minutes on a quarterly basis.

EVIDENCE:
- Calendar entries; documentation of FOCUS Administration meeting minutes pertaining to above procedures as presented by the appointed information security official; company organization chart clearly displaying the appointment of the security official.

RESPONSIBLE PARTY:
- FOCUS Senior Management Team (CEO/CCO/COO)

POLICY:

FOCUS shall appoint security contacts by name for each major organizational area or business unit.0119.05a1Organizational.3 Due to the small size of FOCUS based on the date and version of this policy, the FOCUS Chief Security Officer is assigned this responsibility. In the event that FOCUS grows as an organization and independent business units or departments within the company are created, this policy is subject for review, and when deemed appropriate by FOCUS Administration, security contacts will be appointed by name for each major organizations area or business unit. All annual and quarterly monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to management commitment to information security to determine whether senior management formally appoints security specialists, and review and coordinate results of the specialists' advice throughout the organization.

PROCEDURES:

- The FOCUS Senior Management Team will follow the required policy preceeding this page.
- The FOCUS Chief Security Officer is the security contact for all FOCUS operations and is to be responsible for security in all areas within the company; and
- Should FOCUS grow to warrant appointments of personnel to be security contacts, the FOCUS Chief Security Officer is to appoint said staff.

MONITORING:

- During quarterly FOCUS Senior Management Team meetings, the FOCUS Chief Security Officer will measure and determine if/when FOCUS has grown sufficiently to assign security contacts within organizational areas or business units.

EVIDENCE:

- Quarterly meeting minutes; updating of the FOCUS Security Policy should appointees be named.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

POLICY:

The FOCUS Management Team shall ensure that capital planning and investment requests include the resources needed to implement the security program, employ a business case, and ensure that the resources are available for expenditure as planned.0120.05a1Organizational.4 This is achieved by the **FOCUS Information Protection Program** stipulating that the FOCUS Chief Security Officer is assigned this responsibility with review and approval by the FOCUS CEO. Measurement of success for this FOCUS policy is based on evidence collected by annual review of the **FOCUS budget and expenditure plan for security expenses.** Ongoing quality assurance monitoring mechanisms include semi-annual review of the FOCUS budget and expenditure plan for security expenses by the FOCUS CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:

The FOCUS Chief Security Officer has assigned responsibilities to:

- Utilize the FOCUS RMS Administration system IT Budgeting Module to forecast security related expenditure requests; and
- Develop reasoning/justification for the business case to establish and acquire approval of an annual budget; and
- Hold meetings with FOCUS Management Team to share annual budget requirements; and
- Acquire approval of an annual budget for the fulfillment of the expenditure requests; and
- Document all purchases/acquisitions/fulfillment of the expenditures regarding implementation of the FOCUS Security Program; and
- Report forecasts and utilization of the annual budget to FOCUS Administrators during quarterly administration meetings; and
- If an emergency declaration is made due to natural disaster or security incident requiring unforeseen additional funding to ensure that security measures are in place, the FOCUS CSO coordinates emergency meetings with the FOCUS Management Team to secure resources necessary to ensure security and maintain business operations.

MONITORING:

The FOCUS Chief Security Officer is responsible for:

- Generating the annual budget for security requirements; and
- Posting expenditures against the annual budget to monitor utilization.

EVIDENCE:

- Meeting minutes; approved annual budget; acquisition evidence; implementation documentation; efficacy & assessment of results.

RESPONSIBLE PARTIES:

- FOCUS Management Team
- FOCUS Chief Security Officer

POLICY:
FOCUS shall employ a formal sanctions process for personnel failing to comply with established information security policies and procedures and notifies defined personnel (e.g., supervisors) within a defined time frame (e.g., twenty-four [24] hours) when a formal sanction process is initiated, identifying the individual sanctioned and the reason for the sanction. Further, FOCUS includes specific procedures for license, registration, and certification denial or revocation and other disciplinary action.0135.02f1Organizational.56 This is achieved by educating FOCUS Staff Members in the **FOCUS Code of Conduct** as well as the **FOCUS Security Policy and Procedure** which includes the FOCUS sanctions process and schedule in detail. Further, the FOCUS Review Management System shall have an **'Incident Reporting Function'** to provide all FOCUS Staff Members, Peer Reviewers and client-company end users with an on-screen form within the FOCUS Review Management System to record and report security concerns to the FOCUS CSO to consider application of appropriate sanctions (or reporting of incident to client-companies). Measurement of success for this FOCUS policy is based on evidence collected by attestations from all FOCUS staff members to training on the FOCUS Code of Conduct and FOCUS Security Policy and Procedure. Ongoing quality assurance monitoring mechanisms include annual review of the FOCUS Code of Conduct and FOCUS Security Policy to ensure that sanction information meets regulatory requirements, is accurate and complete. Further, all reported security incidents shall be reviewed within specified policy timeliness standards. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
- It is the responsibility of the FOCUS Chief Security Officer to ensure that the formal sanctions policy and process is incorporated into the FOCUS Code of Conduct document, and is deployed within the FOCUS Review Management system for all FOCUS Staff Members and Peer Reviewers to easily access and read. During mandatory training and document review, the aforementioned stakeholders must attest to understanding and complying with the policy & procedure upon initial hire and annually thereafter; and
- The FOCUS Review Management System provides a splash screen for Employees and contracted Peer Reviewers upon login that explains the importance of security and reveals the sanctions applicable to those who violate the Security Policies; and
- The FOCUS Review Management System provides a submission screen for any/all stakeholders to cite a suspected or actual security violations. Automated notifications are transmitted immediately via text to FOCUS CSO and the Management Team; and
- An alternative mechanism to cite possible or actual infractions is to send an email to: compliance@focushm.com; and
- Upon awareness by any FOCUS Staff Member or contracted Peer Reviewer of suspected or actual non-compliance of FOCUS information security policies and procedures, the FOCUS staff member is required to notify the FOCUS Chief Security Officer (CSO) within one business day and report the suspected or actual infraction; and
- The FOCUS CSO is required to hold a FOCUS Administration meeting which must include at least two other senior staff members with all known information regarding alleged infractions by the Staff Member or Peer Reviewer; and
- Upon agreement by FOCUS Administrators, the Chief Security Officer is to implement formal sanctions process upon the Staff Member or Peer Reviewer which initiated the infraction against FOCUS security policies and procedures as indicated below:

Sanctions
It is the policy of FOCUS Health, Inc. that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. FOCUS Health will categorize violations and impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The sanctions will extend beyond protected health information that is in electronic form and include protected health information in written form. See the violation and sanction tables on page 7 for detailed categorizations of infractions and applicable sanctions. FOCUS Health will take appropriate disciplinary action against employees, contractors, or any individuals who violate FOCUS Health's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

MONITORING:
It is the responsibility of the Chief Security Officer to:
- Present this policy to FOCUS Administration for approval during annual or interim policy review meetings; and
- Schedule annual review of this policy within the company calendar for monitoring; and
- Provide access to all staff and contractors to report suspected or actual infractions to the CSO; and
- Incoming email reports received by the CSO from compliance@focushm.com.

EVIDENCE:
- Meeting minutes, policy approval, policy distribution, policy attestations, personnel files, reported infraction log.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its human resources security protection program (e.g., through policy, standards, guidelines, and procedures).0137.02a1Organizational.3 This is achieved by the **FOCUS Human Resources Security Protection Program** stipulating the purpose, scope, roles, responsibilities, management commitment, coordination and compliance requirements. Measurement of success for this FOCUS Program is based on policies and procedures indicated within the **FOCUS Security Policy and Procedure**. Ongoing quality assurance monitoring mechanisms include semi-annual review by the FOCUS CSO, whereby reports are generated ensuring compliance; and annual review and approval by FOCUS management. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user roles and responsibilities and determine if the organization has developed, disseminated, and annually reviewed/updated a formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. Further, document procedures to facilitate the implementation of the personnel security policy and associated personnel security controls.

PURPOSE
— Insure the security and confidentiality of FOCUS' corporate HR information; and
— Protect against any anticipated threats or hazards to the security and/or integrity of FOCUS' corporate HR; and
— Protect against unauthorized access to or use of FOCUS' HR systems.

SCOPE
— The protection of the confidentiality, integrity and availability of HR information; and
— The development, operation, and administration of the FOCUS Review Management System as a Service platform; and
— The secure operation of communication systems such as chat services, email services and file services.

PROCEDURES:
- It is the responsibility of the FOCUS Chief Security Officer to ensure that FOCUS HR Security policies and procedures are reviewed, presented to the FOCUS Management Team and optimized over time to meet all requirements to preserve and protect HR data.

ROLES
— The FOCUS Chief Security Officer (CSO) is responsible to ensure that all HR data is secure by regularly coordinating efforts with the FOCUS Chief Financial Officer; and
— The FOCUS Chief Financial Officer (CFO) is responsible for entering/modifying/modernizing and maintaining accurate HR data.

RESPONSIBILITIES
— Reminding staff of security importance and possible sanctions in the event of inappropriate data handling is supported via a splash screen which users of the FOCUS Review Management System HR staff is to see daily; and
— Development of 'layman's' version of the FOCUS Security Policy & Procedure for easy consumption, available 24/7/365 to all HR personnel; and
— Semi-Annual frequency of reviewing all security-associated policies, procedures, work plans, job descriptions and personnel files for completeness; and
— Annual training and attestations of all FOCUS policies & procedures applicable to job descriptions, including all security related policies.

MANAGEMENT COMMITMENT
— FOCUS Administrators follow the FOCUS Security Policy & Procedure and fulfill all requirements; and
— For HR Stakeholders to fulfill their obligations and duties as directed within the FOCUS Security Policy & Procedure; and
— To honor and abide by the defined *Purpose, Scope, Roles, Responsibilities and Management Commitment* of the FOCUS HR Security Policy & Procedure.

COORDINATION
— Based on the industry standard 'CIA Triad' of *Confidentiality*, *Integrity* and *Availability:*
  - **Confidentiality** measures are designed to protect against unauthorized disclosure of information.
  - **Integrity** involves protection from unauthorized modifications (e.g., add, delete, or change) of data.
  - **Availability** is protecting the functionality of support systems and ensuring data is fully available at the point in time or period requirements by its users.
— The FOCUS CSO schedules security related topics which are to be incorporated into monthly Administration meetings to ensure compliance.

COMPLIANCE REQUIREMENTS

— LEGAL: The FOCUS CSO conducts monthly compliance research and documents this research and any findings where FOCUS is required by law to comply with HR related requirements. Further the FOCUS CFO is to notify the FOCUS CSO of any and all known legal compliance elements related to HR.

— STAFF: Education for stakeholders including strong passwords, avoiding suspicious emails, maintaining modern software and reporting of unusual behavior on computers.

— PROCESSES: Proactive prevention and quick response in the event of a cybersecurity incident; threat research and prioritization of assets and systems to maintain secure continuity of business.

— TECHNOLOGY: Implementation of tools based on their ability to be integrated and automated to create a Security Fabric that can facilitate the rapid detection and mitigation of threats

MONITORING:

• Monthly FOCUS Administration documented meetings are to include review of policy, discussion regarding new HR Legal Compliance, personnel compliance regarding access, understanding and annual attestation to the policy, modifications to systems as needed to ensure that end-user rules, data exposure and compliance requirements are met or exceeded; entries of all hardware acquisitions and software modifications to ensure safety, security and compliance.

EVIDENCE:

• Meeting minutes; staff attestations to policy; entries into company calendar; hardware acquisition log; software development logs.

RESPONSIBLE PARTY:

• FOCUS Chief Security Officer

SUPPORTING POLICIES AND PROCEDURES:

Location of Supporting Policies: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]

• Training Agenda

SUPPORTING DOCUMENTS:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » SUPPORTING DOCUMENTS » [Document]

• FOCUS Code of Conduct

POLICY

FOCUS shall ensure that individuals are provided mechanisms to make complaints concerning the information security policies, procedures, or FOCUS's compliance with its policies and procedures; documents the complaints and requests for changes, and records their disposition, if applicable.0162.04b1Organizational.2 This is achieved by the **FOCUS Code of Conduct**, which invites FOCUS staff members to report complaints concerning security policies, procedures or compliance matters. The complaint mechanism is available to FOCUS Staff Members 24/7/365 within the FOCUS Review Management System and shall provide categories for selection which include 'Security', 'PII', 'PHI', and 'Management'. Additionally, a special email address has been established for submission as well. Measurement of success for this FOCUS policy is based on evidence collected by attestations where FOCUS Staff Members are given training on how to report concerns in the FOCUS RMS (as documented within the FOCUS Code of Conduct) as well as reports generated by the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include semi-annual review and testing of the reporting mechanism by the FOCUS CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:

- The FOCUS CSO is responsible to ensure that the FOCUS RMS provides a venue, available to all staff and contractors, 24/7/365 for securely and privately documenting any observation, suspicion, or complaint; and
- Alternatively, stakeholders may email the FOCUS Management Team at compliance@focushm.com; and
- The staff member or contractor may choose from multiple categories to classify the comment, and enter free-form text to elaborate as much as desired to explain any and all concerns; and
- The FOCUS CSO and FOCUS COO receives notification that a concern has been posted within the RMS so that the concern may be immediately acknowledged as received by the CSO to the author; and
- The CSO evaluates the concern and report the concern to the FOCUS Management Team. Based on the verification/nature/urgency of the concern, the CSO holds an Administrative meeting within five (5) business days (if justified) or address the concern at the next regularly scheduled Administrative meeting to discuss the concern and take appropriate actions based on input/instructions/guidance of the FOCUS Administrative Team; and
- The CSO is required to respond to the author of the complaint, documented within the RMS; and
- If the complaint is valid and corrections are directed to be made by the FOCUS Administrative Team, a CAP (Corrective Action Plan) to create or modify any policies or procedures are to be authored by the CSO to track all elements to be modified, define deadlines for implementation and track results of the newly implemented policy or procedure modifications.

MONITORING:

- The FOCUS RMS in the Administrative Module is the location of the complaint log so that all members of the FOCUS Administrative team may have access to the complaint, notes/assessments/confirmation of the complaint as well as response to the author of the complaint; and
- The FOCUS CSO is to track all complaints, CAPs, modifications and measure improvement after additions or modifications are implemented.

EVIDENCE:

- Screenshot of the complaint submission system within the RMS (for use by staff or contractors); Screenshot of the complaint processing system within the RMS (for use by FOCUS Administrators); CSO assessment of the complaint; meeting minutes with FOCUS Administrators; final response to the author; semi-annual review of complaints, responses, and consideration of security policy modification(s), if warranted.

RESPONSIBLE PARTIES:

- FOCUS Chief Security Officer
- FOCUS Management Team

SUPPORTING POLICIES AND PROCEDURES:

Location of Supporting Policies: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]

- Training Agenda

SUPPORTING DOCUMENTS:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » SUPPORTING DOCUMENTS » [Document]

- FOCUS Code of Conduct

POLICY:

An independent review of FOCUS's information security management program shall be initiated by management to ensure the continuing suitability, adequacy, and effectiveness of FOCUS's approach to managing information security.0177.05h1Organizational.12 The results of independent security program reviews shall be recorded and reported to the FOCUS Management Team initiating the review; and the results are maintained for a predetermined period of time as determined by FOCUS, but not less than three (3) years.0178.05h1Organizational.3 If an independent review identifies that FOCUS's approach and implementation to managing information security is inadequate or not compliant with the direction for information security stated in the information security policy document, management shall take corrective actions.0179.05h1Organizational.4 This is achieved by the **FOCUS Information Protection Program** stipulating that the FOCUS CSO must contract with an independent vendor to review the FOCUS Information Protection Program annually. Measurement of success for this FOCUS policy is based on reports generated by the independent review vendor. Ongoing quality assurance monitoring mechanisms include semi-annual review of the report by the FOCUS CSO, and confirmation that any recommended modifications are completed as quickly as possible, but no more than 60 days. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the independent review of information security and determine if an independent review of the organization's information security management program is initiated by management to ensure the continuing suitability, adequacy, and effectiveness of the organization's approach to managing information security and privacy. Examine policies and/or standards related to the independent review of information security and determine if the results of independent security program reviews are: (i) recorded and reported to the management who initiated the review; and, (ii) maintained for a predetermined period of time as determined by the organization, but not less than three years.

PROCEDURES:

- The FOCUS CSO Refers to the annual budget to ensure budget compliance for a line-item dedicated to fulfill this requirement, or meets with the FOCUS Management Team to discuss any additional funding required to complete the independent review; and
- The FOCUS CSO identifies and interviews eligible independent review entities, suggests a reviewer to the FOCUS Management Team for final review and selection, contracts with an independent review entity with expertise in reviewing security management programs no less than annually to ensure the continuing suitability, adequacy, and effectiveness of FOCUS's approach to managing information security; and
- The CSO facilitates access to FOCUS policies, procedures and materials required for the assessment to full requirements of the reviewer; and
- The CSO coordinates a results reporting meeting between the independent review vendor and the FOCUS Management Team for thorough review of findings, identification of inadquacies and acquires suggested remedies.
- As needed, the CSO creates Corrective Action Plan (CAP) records located in the RMS » ADMIN » IT » IT CAPS section to begin the remediation tracking process and assigns a deadline for completion with the most high-risk findings to be completed first; and
- Upon receiving the report from the selected independent review entity, all recommendations must be entered into a CAP (Corrective Action Plan) which must include the element(s) in question, current (or new) process(es), recommended change (or creation of) process(es), an agreed to deadline to achieve compliance, and submission of the modification or addition to the review entity for approval of additions or modifications; and
- A follow-up meeting with the independent review entity after CAPs have been remedied to confirm completeness from the reviewers' perspective.
- In the event a CAP for any reason may take more than 60 days to remedy, the CSO schedules a meeting with the FOCUS Management Team to discuss the reason(s) for the delay and to discuss extension of any risks imposed due to the delay; and
- The Independent Review reports are stored within the FOCUS RMS location of RMS » ADMIN » IT » DOCUMENTS for a minimum period of three years; and
- Review of the FOCUS information security management program so that future revisions must take into account all prior assessments to ensure continued compliance and historical CAP recommendations are contained therein.

MONITORING:

The FOCUS CSO budgets time to:

- Add an entry into the FOCUS Calendar to ensure that an independent annual review is conducted annually; and
- Monitor the FOCUS IT Cap Inventory within the FOCUS RMS to ensure that any/all CAPs are being resolved as efficiently as possible; and
- Maintains contact with the prior years' selected independent review vendor so that as CAPs are completed, confirmation of remedy can be attained.

EVIDENCE:

- Meeting minutes; company calendar entries; independent review contract; independent review report.

RESPONSIBLE PARTY: FOCUS Chief Security Officer

URAC C-13	URAC CORE 13; Information Management
0101.00a1Organizational.123	HITRUST 00.a Information Security Management Program
0102.00a2Organizational.123	HITRUST 00.a Information Security Management Program
0104.02a1Organizational.12	HITRUST 02.a Roles and Responsibilities
0107.02d1Organizational.1	HITRUST 02.d Management Responsibilities
0108.02d1Organizational.23	HITRUST 02.d Management Responsibilities
0109.02d1Organizational.4	HITRUST 02.d Management Responsibilities
01110.05a1Organizational.5	HITRUST 05.a Management Commitment to Information Security
0113.04a1Organizational.123	HITRUST 04.a Information Security Policy Document
0114.04b1Organizational.1	HITRUST 04.b Review of the Information Security Policy
0117.05a1Organizational.1	HITRUST 05.a Management Commitment to Information Security
0118.05a1Organizational.2	HITRUST 05.a Management Commitment to Information Security
0119.05a1Organizational.3	HITRUST 05.a Management Commitment to Information Security
0120.05a1Organizational.4	HITRUST 05.a Management Commitment to Information Security
0135.02f1Organizational.56	HITRUST 02.f Disciplinary Process
0137.02a1Organizational.3	HITRUST 02.a Roles and Responsibilities
0162.04b1Organizational.2	HITRUST 04.b Review of the Information Security Policy
0177.05h1Organizational.12	HITRUST 05.h Independent Review of Information Security
0178.05h1Organizational.3	HITRUST 05.h Independent Review of Information Security
0179.05h1Organizational.4	HITRUST 05.h Independent Review of Information Security

02 Endpoint Protection

POLICY:

Anti-virus and anti-spyware shall be installed, operating and updated on all FOCUS end-user devices to conduct periodic scans of the systems to identify and remove unauthorized software. Server environments for which the server software developer specifically recommends not installing host-based anti-virus and anti-spyware software may address the requirement via a network-based malware detection (NBMD) solution.[0201.09j1Organizational.124] FOCUS shall ensure that audit logs of the scans are maintained.[0202.09j1Organizational.3] This is stipulated in the **FOCUS Security Policy and Procedure.** Measurement of success for this FOCUS policy is based on annual review and management approval of the FOCUS Security Policy and Procedure by the CEO and CSO to ensure compliance with this standard. Ongoing quality assurance monitoring mechanisms include quarterly review of the FOCUS Security Policy & Procedure and AV/AM systems by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar. FOCUS shall install and maintain current anti-virus and anti-spyware software.

PROCEDURES:

- The FOCUS CSO evaluates, selects a solution, ensures installation, monitors for consistent utilization, responds to threats, and documents threat occurrances and outcomes.
- All FOCUS end-user devices are to have anti-virus and anti-spyware installed prior to being used in a production setting.
- The FOCUS IT Analysts install the anti-virus and anti-spyware software and initiate the option for automatic scanning and automatic updates of the latest virus/spyware libraries for all end-user devices from the manufacturer.
- The FOCUS IT Analyst(s) monitor for consistent utilization, and notify the FOCUS CSO should a suspected or actual threat be detected.
- The AV/AM vendor is required to generate weekly reports that the FOCUS CSO and FOCUS IT Analyst automatically receive.
- The AV/AM vendor software is required to have a management console for monitoring all endpoints and their status at any time.
- Servers within the FOCUS Co-Location data center(s) where the manufacturer does not recommend AV/AM software installed are to have OSSEC monitoring with automated notifications in the event any operating system or other critical directories are modified so that immediate investigation may be undertaken to ensure security.
- In the event with any risk is found, the FOCUS CSO initiates incident reporting procedures.
- The FOCUS CSO coordinates proper long-term storage of the scan results within the location of: RMS » ADMIN » IT » LOGS » AV/AM Reports.

MONITORING:

- FOCUS CSO records into the FOCUS calendar the requirement of quarterly review of all applicable FOCUS systems to ensure compliance; and
- FOCUS CSO is to enter into company calendar the requirement of annual review and ratification of this policy to ensure compliance.
- FOCUS CSO and FOCUS IT Analyst(s) are to monitor the anti-virus management console to ensure protections are operating fully per the above procedures.

EVIDENCE:

- Company calendar entries; meeting minutes; research notes; manufacturer documentation, automated AV/AM reporting, screen shots of AV/AM management console, automated notification(s).

RESPONSIBLE PARTY:

- FOCUS CSO

VIOLATIONS AND DISCIPLINARY ACTION:

- In the event any FOCUS employee attempts to un-install, modify, delete, or render inoperative in any way, the Anti-Virus/Anti-Malware endpoint software on their workstation will result in disciplinary action(s), including the possibility of termination.

ENFORCEMENT:

- The FOCUS CSO and FOCUS IT Analysts, utilizing the Anti-Virus/Anti-Malware management console, are to review the inventory of end-user systems to ensure that all devices have endpoint software installed, running, and updated with the latest version of anti-virus/anti-malware software on a quarterly basis.

POLICY:

Automated controls (e.g., browser settings) shall be in place to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, and Flash animations).0225.09k1Organizational.1 This is stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on annual review and management approval of the FOCUS Security Policy and Procedure by the CEO and CSO to ensure compliance with this standard. Ongoing quality assurance monitoring mechanisms include quarterly review of the FOCUS Security Policy & Procedure by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:

- The FOCUS IT Analyst manages remote devices with MDM software, and installation of software on workstations is prohibited (including web browser installations for Java, JavaScript, ActiveX, PDF, postscript, Shockwave, etc.); and
- The FOCUS CSO provides training to staff which includes the requirement for end-users to never to attempt installing software on workstations.

MONITORING:

- FOCUS CSO enters into company calendar the requirement of quarterly review of all FOCUS systems to ensure compliance; and
- FOCUS CSO enters into company calendar the requirement of annual review and ratification of this policy to ensure compliance.

EVIDENCE:

- Company calendar entries; meeting minutes; training attestations.

RESPONSIBLE PARTY:

- FOCUS IT Analyst

POLICY:

FOCUS has implemented and regularly updates mobile code protection, including anti-virus and anti-spyware.[0226.09k1Organizational.2] This is stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on annual review and management approval of the FOCUS Security Policy and Procedure by the CEO and CSO to ensure compliance with this standard. Ongoing quality assurance monitoring mechanisms include quarterly review of the FOCUS Security Policy & Procedure by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: As of the effective date of this policy, FOCUS prohibits and prevents mobile software or access to FOCUS systems.

PROCEDURES:

- As of the effective date of this policy, FOCUS prohibits and prevents mobile software or access to FOCUS systems; and
- In the event FOCUS initiates use of mobile 'apps', this policy will be revised to address meeting this requirement.

MONITORING:

- FOCUS CSO enters into company calendar the requirement of quarterly review of all FOCUS systems to ensure compliance; and
- FOCUS CSO enters into company calendar the requirement of annual review and ratification of this policy to ensure compliance.

EVIDENCE:

- Company calendar entries; meeting minutes; research notes.

RESPONSIBLE PARTY:

- FOCUS IT Analyst

POLICY:
FOCUS ensures that protection against malicious code is based on malicious code detection and repair software, security awareness, and appropriate system access and change management controls.[0214.09j1Organizational.6] This is stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on annual review and management approval of the FOCUS Security Policy and Procedure by the CEO and CSO to ensure compliance with this standard. Ongoing quality assurance monitoring mechanisms include quarterly review of the FOCUS Security Policy & Procedure by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.
NOTE: As of the effective date of this policy, FOCUS prohibits and prevents mobile software or access to FOCUS systems.

PROCEDURES:
- As of the effective date of this policy, FOCUS prohibits and prevents mobile software or access to FOCUS systems; and
- In the event FOCUS initiates use of mobile 'apps', this policy will be revised to address meeting this requirement.

MONITORING:
- FOCUS CSO enters into company calendar the requirement of quarterly review of all FOCUS systems to ensure compliance; and
- FOCUS CSO enters into company calendar the requirement of annual review and ratification of this policy to ensure compliance.

EVIDENCE:
- Company calendar entries; meeting minutes; research notes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 02 ENDPOINT PROTECTION

0201.09j1Organizational.124	HITRUST 09.j Controls Against malicious Code
0202.09j1Organizational.3	HITRUST 09.j Controls Against malicious Code
0225.09k1Organizational.1	HITRUST 09.k Controls Against Mobile Code
0226.09k1Organizational.2	HITRUST 09.k Controls Against Mobile Code
0214.09j1Organizational.6	HITRUST 09.j Controls Against malicious Code

03 Portable Media Security

POLICY:
FOCUS, based on the data classification level, shall register media (including laptops) prior to use, places reasonable restrictions on how such media be used, and provides an appropriate level of physical and logical protection (including encryption) for media containing covered information until properly destroyed or sanitized.0301.09o1Organizational.123 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **system inventory reports**, **end-user training**, and **screen-shots of system management software** which are stored in the FOCUS Review Management System and reviewed annually by the CSO. Ongoing quality assurance monitoring mechanisms include evidence collected by **system inventory reports**, which are monitored quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.
FOCUS provides remote workstation sessions so that all covered information remains in the possession of FOCUS and on FOCUS servers.

FOCUS shall examine policies and/or standards related to the management of removable media and determine if the organization formally establishes and enforces controls (e.g., policies and procedures) for the management of removable media and laptops including: (i) restrictions on the type(s) of media, and usages thereof to maintain security; and, (ii) registration of certain type(s) of media including laptops. Media containing covered information is physically stored and its data encrypted in accordance with the organization's data protection and privacy policy on the use of cryptographic controls (see 06.d) until the media are destroyed or sanitized (see 09.p) and commensurate with the confidentiality and integrity requirements for its data classification level.

NOTE: As of the effective date of this policy, FOCUS prohibits storing any covered (confidential) information by any user on Portable Media (including laptops) or desktop workstations.

The following procedures are intended to meet the above policy requirements regarding the remaining elements:

PROCEDURES:

The use of transportable/portable media provides an ease of storing and transmitting data. However, preventative measures must be in place to provide for the assurances that the data contained on those devices are protected and do not contain information of a confidential nature.

- All acquired FOCUS devices must be catalogued within the RMS Administration section for inventory, and each item must be assigned a data classification level *prior to use*; and
- All FOCUS portable media devices (laptops) are to be configured for full-disk encryption; and
- Users are provided training (which requires attestation) to understand that they are prohibited from ever storing 'covered information' (e.g., PHI/PII) on the device; and
- Users are prohibited from connecting their transportable/portable media to a workstation that is issued by or owned by any other entity; and
- When an employee concludes their employment at FOCUS or if the device is returned to FOCUS for replacement, all transportable/portable media in their possession must be returned to the Chief Security Officer or IT Analyst for proper data erasure and documentation thereof.

MONITORING:
- Quarterly portable media inventory reports, quarterly meetings with documented meeting minutes detailing the current utilization and locations of any portable media, annual review of the portable media security policy.

EVIDENCE:
- Portable media inventory reports; meeting minutes, screenshot of portable media inventory tracking system, end user training attestations.

RESPONSIBLE PARTY:

- FOCUS IT Analyst

SUPPORTING POLICIES & PROCEDURES:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]

- FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS media shall be labeled, encrypted, and handled according to its classification.0305.09q1Organizational.12 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **media inventory reports**, **data wiping reports**, **destruction logs** and **photographic evidence of physical media destruction** which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include evidence collected by **system inventory reports**, which are monitored quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information handling to determine if procedures for handling, processing, communication and storage of information (including information media awaiting disposal) is established to protect data from unauthorized disclosure or misuse including: (i) physical and technical access restrictions commensurate with the data classification level, and (ii) handling and labeling of all media according to its indicated classification (sensitivity) level.

NOTE: As of the effective date of this policy, FOCUS prohibits storing any covered (confidential) information by any user on Portable Media (including laptops) or desktop workstations. Further, FOCUS does not utilize server-based backup technology based on 'tape' media.

PROCEDURES:
All FOCUS portable media devices (laptops) are to:
- Be physically labeled for identification according to its classification; and
- Configured for full-disk encryption; and
- Be configured with MDM software to prohibit access to USB or other I/O ports for external portable media; and
- Handled according to its classification, including data wiping reports, destruction logs and photographic evidence of physical media destruction to be stored in the following location: RMS » ADMIN » IT » INVENTORY; and
- Documented within the following location: RMS » ADMIN » IT » INVENTORY.

MONITORING:
- Annual review of the FOCUS portable media policy;

EVIDENCE:
- Annually ratified portable media policy; screenshot of FOCUS IT inventory system; inventory reports; physical media data wiping reports; destruction logs; photographic evidence of destruction.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

SUPPORTING POLICIES & PROCEDURES:
Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]
- FOCUS Storage & Destruction Policy

POLICY:
The status and location of unencrypted covered information shall be maintained and monitored by FOCUS.0306.09q1Organizational.3 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **unencrypted covered information inventory reports**, and **whole disk encryption system inventory reports**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include evidence collected by **unencrypted covered information inventory reports**, which are monitored quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information handling to determine if procedures for handling, processing, communication and storage of information (including information media awaiting disposal) is established, monitored, and enforced to protect data from unauthorized disclosure or misuse including, monitoring the status and location of media containing unencrypted covered information.

NOTE: It is the policy of FOCUS to always have covered information encrypted (in transport and at rest).

PROCEDURES:
The FOCUS CSO ensures that:
• All media is encrypted so as to ensure that all 'covered information' (e.g., PHI/PII) is always encrypted; and
• Inventory reports must be generated to demonstrate that whole disk encryption is in place for all devices; and
• Covered information is always encrypted during transport.

MONITORING:
The CSO ensures that:
- Company calendar entries are made so as to ensure annual review of this policy; and
- Quarterly reviews to confirm that all media is encrypted, based on review, confirmation, and documentation of all systems; and
- Each quarter, the CSO is to generate meeting minutes to illustrate the review, confirmation and documentation of encryption.

EVIDENCE:
- Company calendar entries; report of documented review of all systems; meeting minutes; whole disk encryption reports.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 03 PORTABLE MEDIA SECURITY

0301.09o1Organizational.123	HITRUST 09.o Management of Removable Media
0305.09q1Organizational.12	HITRUST 09.q Information Handling Procedures
0306.09q1Organizational.3	HITRUST 09.q Information Handling Procedures

04 Mobile Device Security

POLICY:
Mobile computing devices shall be protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls, or equivalent functionality, secure configurations, and physical protections.0401.01x1System.124579

NOTE: FOCUS Health prohibits the use of cell phones and tablets to directly access the FOCUS network. However, web browser based access from phones and tablets is permitted.

PROCEDURES:
The FOCUS CSO ensures that:
- The FOCUS IT Analyst configures the Cisco ASA Firewall to only allow external internet web browser traffic to FOCUS RMS web servers via port 443 with secure socket layer (SSL) certificates for non-employee stakeholders accessing the FOCUS RMS via a web browser (authorized contracted Peer Reviewers and authorized client-company end-users); and
- The FOCUS IT Analyst responsible for establishing VPN access for employees is prohibited from providing any non-employee user with VPN access to the FOCUS network; and
- VPN access is to only be provided to FOCUS employees as part of FOCUS' baseline configuration on their remote, FOCUS provided, desktop or laptop workstation; and
- The privilege sets and access controls are reviewed on a quarterly basis to ensure security.

MONITORING:
The CSO ensures that:
- Quarterly monitoring, documented by meeting minutes, of external web browser users and their privilege sets; and
- Annual review/edit/ratification of this policy to ensure compliance.

EVIDENCE:
- Company calendar entries; meeting minutes detailing quarterly audit of external web browser based user privileges.

RESPONSIBLE PARTY:
- FOCUS CSO

SUPPORTING POLICIES & PROCEDURES:
Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]
- FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS ensures that mobile computing devices are protected at all times by access controls, usage restrictions, connection requirements, encryption, virus protections, host-based firewalls or equivalent functionality, secure configurations, and physical protections.0401.01x1System.124579 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **access controls (remote disconnection from employee computer; access privileges revoked from the FOCUS RMS); attestations of FOCUS policies and procedures by FOCUS staff and Peer Reviewers;** and **firewall rules**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar. Further, mobile device usage for illegal or dangerous activity, for purposes of harassment, or in ways that violate the company confidentiality policy may result in employee termination.

PROCEDURES:
The FOCUS CSO ensures that:
- Access controls are in place by the use of VPN access through FOCUS' security appliance as well as two-factor authentication upon accessing the FOCUS Review Management System (the singular data system where all FOCUS covered information is maintained); and
- Additional access controls are in place, centrally managed by tools deployed to FOCUS IT Analysts, to prevent unauthorized features or functions on the mobile device; and
- Usage restrictions, in the form of privilege sets to control access to FOCUS data; and
- Usage restrictions, in the form of end-user training with instructions which state that *'mobile device usage for illegal or dangerous activity, for purposes of harassment, or in ways that violate the company confidentiality policy may result in employee termination.';* and
- Connection requirements, as stipulated in end-user training with instructions on *acceptable* and *unacceptable* connections such as networking, printers, storage or other devices; and
- Encryption of internal storage, which is required before deployment to any end-user, as well end-user training regarding the prohibition of the use of removable media; and
- Virus protections (in the future event that FOCUS deploys non-BSD based operating systems) FOCUS IT Staff are to install virus and anti-malware software, and training will be provided to end-users to ensure that virus protection tools are to never be disabled or circumvented at any time; and
- The appropriate IT staff member is to ensure that Host-based firewall software, built into every Macintosh operating system (MacOS), is to be activated and prevent discontinuance from the mobile device; and
- The appropriate IT staff member is to ensure that configuration of all mobile devices are secure.
- Physical protections are defined in the FOCUS 'Mobile Device Policy v1.0.pdf'; and
- FOCUS IT Analysts are to maintain remote management software so that mobile devices may be remotely erased, locked or disabled if the CSO determines that there is risk of data loss for any reason.

MONITORING:
The CSO ensures that:
- The company calendar has entries for annual and quarterly monitoring events; and
- Quarterly monitoring, documented by meeting minutes, of *access controls, usage restrictions, connection requirements, encryption, virus protections, host based firewalls and physical protections* are audited within the FOCUS RMS Administration/IT inventory tracking system; and
- Annual review/edit/ratification of this policy to ensure compliance.

EVIDENCE:
- Company calendar entries; meeting minutes detailing annual approval of policy; meeting minutes detailing quarterly audit activities of system inventory.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall monitor for unauthorized connections of mobile devices.[0403.01x1System.8] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **training and acknowledgement evidence of FOCUS staff members and Peer Reviewers;** and **firewall logs**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO and monthly by the FOCUS IT Analyst. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
- The FOCUS IT Analyst configures the Cisco ASA Firewall to only allow external internet web browser traffic to FOCUS RMS web servers via port 443 with secure socket layer (SSL) certificates for non-employee stakeholders accessing the FOCUS RMS via a web browser (authorized contracted Peer Reviewers and authorized client-company end-users); and
- The FOCUS IT Analyst configures the Cisco ASA Firewall to prohibit and prevent access to the RMS from the external network (internet) via any port other than 443 (above); and
- The RMS 'activity log' is reviewed monthly to confirm that users (other than FOCUS employees) are utilizing web browsers to access the FOCUS system.

MONITORING:
- The FOCUS CSO is to enter calendar entries to review this policy annually for renewal and ratification; and
- The FOCUS CSO is to review the activity log on a monthly basis; and
- The FOCUS CSO is to confirm proper configuration of the ASA firewall by demonstration and documented evidence; and

EVIDENCE:
- Calendar entries for annual review of this policy; calendar entries for quarterly and weekly review of the unapproved device log; screen shot of the on-screen notification to and end user utilizing an unapproved device.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that specially configured mobile devices are issued for personnel traveling to high risk locations and are checked for malware and physical tampering upon return.0404.01x1System.1011 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by a FOCUS IT Analyst and entry of mobile device assignment within the FOCUS IT Inventory System**.** This policy shall be reviewed and ratified annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of the IT inventory system quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
Any FOCUS Employee that is required to travel with company provided mobile devices is required to:
- Notify the FOCUS CSO in advance of traveling; and
- Upon approval of taking company mobile devices by the CSO, the traveler is to be provided a specially configured mobile device by a FOCUS IT Analyst; and
- The FOCUS IT Analyst must document who was given the device, on what date, at what time, and when return is estimated; and
- The device must be delivered within three (3) business days upon returning from traveling to the FOCUS IT Analyst; and
- The FOCUS IT Analyst must inspect the device for malware and physical tampering upon return; and
- Update the FOCUS RMS Administrative/IT Inventory system that the device has been inspected and returned.

MONITORING:
- The FOCUS CSO creates calendar entries for annual review of this policy.
- The FOCUS CSO monitors the IT inventory system quarterly with documented meeting minutes.

EVIDENCE:
- IT Inventory logs; calendar entries; annual renewal of policy; IT Inventory Reports; meeting minutes.

SUPPORTING POLICIES & PROCEDURES:
Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]
- FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS shall ensure that teleworking activities of FOCUS Staff and Peer Reviewers are only authorized if security arrangements and controls that comply with relevant security policies and organizational requirements are in place.0405.01y1Organizational.12345678 These requirements are stipulated in the **FOCUS Security Policy and Procedure** and the **Mobile Device Policy**. Due to FOCUS being a virtual company, all users must be trained on, read, acknowledge understanding through attestation and abide by these policies. Measurement of success for this FOCUS policy is based on evidence collected by **training and acknowledgement evidence of FOCUS staff members** for both policies**;** and that **VPN access to FOCUS systems is required;** and **that ethernet connectivity is required,** which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to teleworking and determine if the following teleworking arrangements exist: (i) teleworking activities are formally managed/controlled and only authorized if suitable security arrangements and security controls that comply with relevant security policies and organizational requirements are in place; (ii) the communications security requirements are addressed and take into account the need for remote access to the organization's internal systems, the sensitivity of the information that will be accessed and pass over the communication link and the sensitivity of the internal system.; (iii) the use of home networks and requirements/restrictions on the configuration of wireless network services including encryption (AES WPA2 at a minimum) are addressed; (iv) antivirus protection, operating system and application patching, and firewall requirements consistent with corporate policy are addressed; (v) revocation of authority and access rights and the return of equipment when the teleworking activities are terminated are addressed; (vi) verifiable unique IDs are required for all teleworkers accessing the organization's network via a remote connection; (vii) the connection between the organization and the teleworker's location is secured via an encrypted channel; and, (viii) the organization maintains ownership over the assets used by the teleworker in order to achieve the requirements of this control.

PROCEDURES:
The FOCUS CSO ensures that:
- The FOCUS Mobile Device Policy is reviewed, edited, and ratified at least annually; and
- The FOCUS Onboarding Policy (including Mobile Device Policy training) is provided to new hires prior to accessing FOCUS systems, and annually thereafter, to all Staff Members and contracted Peer Reviewers; and
- Upon moving to a new location, Employees must re-certify their work environment; and
- A review with approval or denial of teleworking for each FOCUS employee or contracted Peer Reviewer based on:
  - The work environment (a private location to conduct FOCUS business); and
  - Physical security (lockable residence or facility doors); and
  - A FOCUS employee having a wired ethernet cable to connect their FOCUS provisioned computer to the internet.

MONITORING:
The FOCUS CSO:
- Enters calendar records for annual review of the FOCUS Mobile Device Policy; and
- Monitors training evidence to ensure that all new hires and existing Staff Members and Peer Reviewers complete training and attestations before accessing FOCUS systems remotely.

EVIDENCE:
- Company calendar entries; meeting minutes when ratifying policies; training attestations; CSO authorizations for new hires

RESPONSIBLE PARTY: FOCUS Chief Security Officer

SUPPORTING POLICIES & PROCEDURES: Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS shall provide a documented list of approved application stores has been defined as acceptable for mobile devices accessing or storing entity (client) or cloud service provider-managed client data, and the use of unapproved application stores is prohibited for company-owned and BYOD mobile devices. Non-approved applications or approved applications not obtained through approved application stores are prohibited.[0425.01x1System.13] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **training and acknowledgement evidence of FOCUS staff members;** and **screenshot showing denial of attempted software installation by an end user**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: Installing applications on FOCUS Systems (other than by FOCUS IT Team Members) is prohibited and prevented.

PROCEDURES:
The FOCUS CSO ensures that:
- Training regarding the process of requesting software is provided to all FOCUS Staff Members, and that all trainees must read, attest and abide by this policy; and
- Any application not included in the FOCUS baseline system configuration being requested for installation on FOCUS workstations is researched, tested on equipment isolated from Covered Information, and only installed after authorization by the CSO has been completed.; and
- MDM endpoint configuration settings must prevent installation of all applications; and
- At no time are unauthorized cloud based services be permitted; and
- All requests by an Employee and the resulting approval or denial for software by the CSO will be documented in the RMS location of: RMS » ADMIN » IT » INVENTORY.

MONITORING:
- Calendar entries for policy review, renewal and ratification; and
- Review of the FOCUS Administration System/IT Inventory of requests, denials and approvals.

EVIDENCE:
- Company calendar entries; training logs; policy renewals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

SUPPORTING POLICIES & PROCEDURES:
Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]
- FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS shall prohibit the circumvention of built-in security controls on mobile devices (e.g., jailbreaking or rooting).0429.01x1System.14 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **training and acknowledgement evidence of FOCUS staff members and Peer Reviewers;** and **screenshot showing configuration of a device for a FOCUS staff member**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: FOCUS prevents and prohibits mobile phones and tablets from connecting to the FOCUS network.

PROCEDURES:
- The FOCUS CSO ensures that training regarding the prohibition of intentionally circumventing the built-in security controls on mobile devices is provided to all FOCUS Staff Members, and that all trainees must read, attest and abide by this policy.

MONITORING:
- The FOCUS CSO schedules to review, update and ratify this policy on an annual basis; and
- The FOCUS CSO reviews training and attestation records to ensure participation and compliance.

EVIDENCE:
- Company calendar entries; training logs; policy renewals; Mobile Device Management Logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

SUPPORTING POLICIES & PROCEDURES:
Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]
- FOCUS Telecommuter Confidentiality Policy

POLICY:
If it is determined that encryption is not reasonable and appropriate, FOCUS documents its rationale and acceptance of risk.0410.01x1System.12 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by s**ecure certificates utilized by FOCUS servers;** and **screenshots showing evidence that no TCP/IP ports are open on the firewall,** and **screenshots of VPN security**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that transport, distribution and storage of protected data (PHI/PII) shall always be encrypted, both at rest and in transit.

PROCEDURES:
FOCUS CSO ensures that:
- Per FOCUS policy, transport, distribution and storage of protected data (PHI/PII) is always to be encrypted, both when at rest and in transit; and
- Any stakeholder that wishes to request an exception to this policy must contact the FOCUS CSO and submit a request; and
- The FOCUS Management Team must meet with the CSO, review all risks, record meeting minutes, and approve (or deny) the request; and
- If a request is ever granted by the FOCUS Management Team, the exception must be documented, with rationale, and this policy must be amended and ratified; and
- The CSO will document the exception in the RMS location of: RMS » ADMIN » IT » INVENTORY.

MONITORING:
- The FOCUS CSO reviews, update and ratify this policy on an annual basis; and
- The FOCUS CSO reviews, on a quarterly basis, the FOCUS IT Management inventory of all unencrypted covered data elements and ensure that rationale is documented; and
- The FOCUS CSO, on a quarterly basis, must contact the originating requestor and confirm the continued need for unencrypted Covered Information; and
- Once it is no longer necessary for the Covered Information to be unencrypted, the FOCUS CSO will take steps to ensure encryption.

EVIDENCE:
- Secure certificate verification documents; firewall port configuration screenshots; VPN security screenshots; CSO authorization of unencrypted data elements and accompanying acceptance of risk.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that suitable protections of the teleworking site are in place to protect against the theft of equipment and information, the unauthorized disclosure of information, and unauthorized remote access to FOCUS's internal systems or misuse of facilities.[0415.01y1Organizational.10] These requirements are stipulated in the **FOCUS Security Policy and Procedure** and the **FOCUS Mobile Device Policy**, the **FOCUS HIPAA Policy**, and the **FOCUS Confidentiality of Personal Health Information (PHI) Policy**. Measurement of success for this FOCUS policy is based on evidence collected by **training and acknowledgement evidence of FOCUS staff members and Peer Reviewers;** and **screenshots illustrating remote system lock and remote system erasure;** and **FOCUS confidentiality agreements** with **acknowledgement evidence of FOCUS staff members and Peer Reviewers**, and **screenshot illustrating WiFi services are disabled on staff computers**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence monthly by the CSO and IT Analysts. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FH is a 'virtual' company that has no physical facility where all stakeholders unite to work. To support this business model, all FH staff members work remotely. However, there are limits and requirements which must be adhered to in an effort to maximize security of company data.

PROCEDURES:
- The FOCUS CSO ensures that the FOCUS Mobile Device Policy is reviewed/modified/ratified annually; and
- All FOCUS Staff Members and Peer Reviewers must read, attest, and comply with the FOCUS Mobile Device Policy; and
- The FOCUS CSO ensures that the FOCUS HIPAA Policy is reviewed/modified/ratified annually; and
- All FOCUS Staff Members and Peer Reviewers must read, attest, and comply with the FOCUS HIPAA Policy; and
- The FOCUS CSO ensures that the FOCUS Confidentiality of Personal Health Information (PHI) Policy is reviewed/modified/ratified annually; and
- All FOCUS Staff Members and Peer Reviewers must read, attest, and comply with the FOCUS Confidentiality of Personal Health Information (PHI) Policy; and
- The FOCUS CSO and FOCUS IT Analysts ensures that the Security Appliance (hardware firewall) where all FOCUS data is stored and served is inspected, logs reviewed, configuration(s) confirmed and tested to prevent unauthorized remote access to internal systems or misuse.
- Computers must be kept in a work or home office; and
- Computers must only be accessed by the FH staff member or peer reviewer; and
- Employees must be isolated in a room designated for work to be performed with an attached door; and
- Wireless access is not permitted for FOCUS Employees; connection to the internet via Ethernet cable is required; and
- At no time should any employee provide their login or email password to anyone, not even family members; and
- At no time should the computer in use be connected simultaneously to any other network; and
- All remote users with Windows computers must have the most up-to-date virus protection activated.
- Laptop computers may not be removed from the designated place of work; and
- Access to company systems (the RMS) is not allowed on public computers (library, etc.); and
- Access to company systems (the RMS) is not allowed on any other users' computer (friend, etc.).
- All FOCUS network technology and data systems will require authentication.

NOTE: non-compliance of the FH Security Policies and Procedures potentially constitute grounds for immediate termination.

MONITORING:
- All policy reviews are to be entered into the company calendar by the CSO for annual review; and
- All inspections of the Security Appliance are to be entered into the company calendar by the CSO for monthly inspections; and
- The FOCUS CSO is to review the above policies no less than annually; and
- The CSO is to review training logs monthly to ensure that all new hires and annual staff training thereafter contain attestations by all users of FOCUS systems.

EVIDENCE:
- Training attestations; calendar entries; active policies; Security Appliance logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

SUPPORTING POLICIES & PROCEDURES:

Location of Supporting Documents: RMS » ADMIN » ORGANIZATION » P&Ps » [Document]

- FOCUS Confidentiality of Personal Health Information (PHI) Policy
- FOCUS HIPAA Policy
- FOCUS Mobile Device Policy

REFERENCED STANDARDS FOR 04 PORTABLE MEDIA SECURITY

0401.01x1System.124579	HITRUST 01.x Mobile Computing and Communications
0403.01x1System.8	HITRUST 01.x Mobile Computing and Communications
0404.01x1System.1011	HITRUST 01.x Mobile Computing and Communications
0405.01y1Organizational.12345678	HITRUST 01.y Teleworking
0425.01x1System.13	HITRUST 01.x Mobile Computing and Communications
0429.01x1System.14	HITRUST 01.x Mobile Computing and Communications
0410.01x1System.12	HITRUST 01.x Mobile Computing and Communications
0415.01y1Organizational.10	HITRUST 01.y Teleworking

05 Wireless Security

POLICY:
Vendor defaults for wireless access points shall be changed by FOCUS IT Analysts prior to authorizing the implementation of the access point.[0501.09m1Organizational.1] Wireless access points shall be configured with strong encryption (AES WPA2 at a minimum) by FOCUS IT Analysts.[0502.09m1Organizational.5] Wireless access points are placed in secure locations by FOCUS IT Analysts.[0503.09m1Organizational.6] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **screenshots of WiFi configuration software**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the management of wireless access points and determine if when configuring wireless access points and devices, the organization changes the following: (i) vendor default encryption keys; (ii) encryption keys anytime anyone with knowledge of the keys leaves the company or changes positions; (iii) default SNMP community strings on wireless devices; (iv) default passwords/passphrases on access points; and, (v) other security-related wireless vendor defaults, if applicable.

FOCUS shall examine policies and/or standards related to the management of wireless access points and determine if wireless access is explicitly approved, wireless access points and devices have appropriate (e.g., FIPS-approved; minimum of AES WPA2) encryption enabled for authentication and transmission.

NOTE: It is FOCUS policy that no wireless access points are provided by the company.

PROCEDURES:
- The FOCUS CSO ensures that this policy is reviewed/modified/ratified annually; and
- It is FOCUS policy that no wireless access points are provided by the company; and
- In the event that FOCUS business requirements change, and wireless access points become a required network element, the FOCUS Management Team and the FOCUS CSO are required to conduct needs analysis, risk analysis and conduct formal and documented meetings with rationale to reverse the current 'no wireless access points' policy; followed by modification of this policy and include all safeguards in accepting the management, encryption and use of wireless access.

MONITORING:
- The FOCUS CSO is to review this policy and edit/modify/ratify annually; and
- The FOCUS CSO is to review the FOCUS IT Administration/IT Inventory tracking system for WiFi hardware and/or activated systems wifi activation and reception to ensure compliance.

EVIDENCE:
- If wireless access hardware exists in the future, screenshots of configuration screen(s) shall be on file.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 05 WIRELESS SECURITY

0501.09m1Organizational.1	HITRUST 09.m Network Controls
0502.09m1Organizational.5	HITRUST 09.m Network Controls
0503.09m1Organizational.6	HITRUST 09.m Network Controls

06 Configuration Management

POLICY:
Annual compliance reviews shall be conducted by the FOCUS CSO using manual or automated tools; if non-compliance is found, appropriate action is taken.0601.06g1Organizational.124 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **independent penetration testing,** and the **FOCUS risk assessment report**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the compliance of security policies and standards to determine if compliance reviews are conducted by security, privacy and/or audit individuals and will incorporate reviews of documented evidence. Annual compliance assessments are conducted and, if any non-compliance is found as a result of the review, managers will: (i) determine the causes of the non-compliance; (ii) evaluate the need for actions to ensure that non-compliance do not recur; (iii) determine and implement appropriate corrective action; and, (iv) review the corrective action taken. Automated tools are used where possible, but manual processes are acceptable.

PROCEDURES:
- The FOCUS CSO ensures that this policy is reviewed/modified/ratified annually; and
- The FOCUS CSO conducts an annual audit meeting composed of the CSO and FOCUS IT Analysts to:
  - Review policies, review security appliance logs, review systems configurations; and
  - Confirm that all users have attested to all training, review IT inventory to ensure compliance; and
  - Review FOCUS Security Policy & Procedure and assess compliance with all policies therein; and
  - The FOCUS Analysts, using IT tools to assess network accessibility and security compliance, are to generate reports from these tools and present the reports to the CSO during the annual meeting with results.
- If non-compliance is found, the FOCUS CSO documents this within the meeting minutes and gives documented instructions detailing the corrective action plan to correct non-compliance.

MONITORING:
- The FOCUS CSO is to review this policy and edit/modify/ratify annually; and
- The FOCUS CSO is to create entries within the company calendar for IT Analyst security tools to generate reports; and
- The FOCUS CSO is to create entries within the company calendar for the annual compliance review; and
- Hold the annual compliance review meeting and document the meeting and outcomes in meeting minutes.

EVIDENCE:
- Calendar entries; meeting minutes; corrective action plan, active policy, security tool reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The results and recommendations of the reviews shall be documented and approved by FOCUS management.0602.06g1Organizational.3 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **FOCUS IT meeting minutes** documenting the analysis of **independent penetration testing,** and the **FOCUS risk assessment report**, **documenting any identified issues** and **resolution to issues identified**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— A company calendar entry is made to by he CSO to present the compliance review findings to the FOCUS Administrative Team annually; and
— The results and recommendations of the reviews are presented, documented within meeting minutes and approved by the FOCUS Administrative Team.

MONITORING:
- A company calendar entry is made by the CSO to present the compliance review findings to the FOCUS Administrative Team annually.

EVIDENCE:
- Company calendar entries; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Only authorized FOCUS IT Analysts shall be allowed to implement approved upgrades to software, applications, and program libraries, based on business requirements and the security implications of the release.[0605.10h1System.12] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **attestations from the CSO and all FOCUS IT Analysis staff members,** and where policy states that **upgrades are prohibited by unauthorized personnel**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the control of operational software to determine if the updating of the operational software, applications, and program libraries is performed by authorized administrators and operational systems that only hold approved programs or executable code (i.e., no development code or compilers). Any decision to upgrade to a new release takes into account the business requirements for the change, and the security and privacy impacts of the release (e.g., the introduction of new security functionality or the number and severity of security problems affecting this version).

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— FOCUS Staff Members and Peer Reviewers are provided training and must attest to understanding that they are not to attempt to install applications, patches to any FOCUS system on their own; and
— The FOCUS CSO requires FOCUS IT Analysts to identify and document upgrades (patches, application updates, program libraries) and enter them into the FOCUS Administration module/IT Inventory system for CSO approval; and
— The FOCUS CSO requires the FOCUS IT Analysts to apply documented upgrades to test equipment to evaluate the security, functionality and stability of upgrades before applying upgrades to production systems (within 48 hours, if approved); and
— Only FOCUS IT Analysts are allowed to implement approved upgrades to software, applications and program libraries; and
— The FOCUS IT Analysts are to document the version numbers and upgrade history for each device within the FOCUS Administration module/IT Inventory system.

MONITORING:
- The FOCUS CSO is to monitor the FOCUS Administration module/IT Inventory system for outstanding updates/patches/application requests on a monthly basis and provide oversight and instructions to FOCUS IT Analysts regarding security and stability testing and approval of upgrades/applications or other required patches or requests; and
- The FOCUS CSO is to monitor the FOCUS Administration module/IT Inventory system for completed installations/upgrades.

EVIDENCE:
- Calendar entries; screenshot of IT inventory system with requests, approvals and completed tasks.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS IT Analysts shall ensure that computing hardware operating systems have supporting technical controls such as antivirus, file integrity monitoring, host-based (personal) firewalls or port filtering tools, and logging as part of its baseline.0663.10h1System.7 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **end user training with attestations** regarding the use of the **PHI security reporting system** documenting occurrences of inappropriate presence of PHI, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Further, **system inventory reports** illustrating **firewalls**, **port filtering** and **logging** must be stored in the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— Please refer to FOCUS policy *0201.09j1Organizational.1245* regarding antivirus and anti-spyware; and
— FOCUS systems are to have file integrity monitoring logs stored within the FOCUS Administrative module/IT Inventory from the database server; and
— Each FOCUS system (both servers and end-user systems) is to have host-based firewalls and port filtering activated to reduce communications to minimum requirements to fulfill user responsibilities; and
— The FOCUS RMS generates, and FOCUS IT Analysts store, a comprehensive log of all activity within the FOCUS Administrative module/IT Inventory system.

MONITORING:
- The FOCUS CSO monitors the FOCUS Administration module/IT Inventory system for outstanding updates/patches/application requests on a monthly basis and provide oversight and instructions to FOCUS IT Analysts regarding security and stability testing and approval of upgrades/applications or other required patches or requests; and
- The FOCUS CSO monitors the FOCUS Administration module/IT Inventory system for completed installations/upgrades.

EVIDENCE:
- Current policy & procedure; company calendar entries; file integrity monitoring logs; screenshot of host-based firewall configurations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall perform annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools, and takes appropriate action if non-compliance is found.0613.06h1Organizational.12 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **independent penetration testing, FOCUS business continuity tests** and **review of FOCUS risk assessments** are conducted and monitored annually by the CSO. Further, the above documents and reports must be stored in the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to technical compliance checking to determine if the organization performs annual checks on the technical security configuration of systems, either manually by an individual with experience with the systems and/or with the assistance of automated software tools. If any non-compliance is found as a result of a technical security configuration compliance review, the organization: (i) determines the causes of the non-compliance; (ii) evaluates the need for actions to ensure that non-compliance do not recur; (iii) determines and implements appropriate corrective action; and, (iv) reviews the corrective action taken.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— An expert in penetration testing (vendor) is to be contracted, including executed non-disclosure agreement, to test FOCUS systems no less than annually; and
— FOCUS acquires the report from the vendor and review findings; and
— Identify any identified security issues (High, Medium and Low) and implement a corrective action plan; and
— Oversee the corrective action plan to ensure that all identified security issues are corrected within thirty (30) days; and
— A subsequent scan from the vendor is to be run to provide evidence that any HIGH or MEDIUM security issues identified in the initial report are 100% mitigated; and
— Based on the subsequent scan, any LOW security issues are explained within documentation as to their exact nature, why they cannot be mitigated (if applicable) or when they are expected to be mitigated through future patches/updates, etc.; and
— Assignment of an appropriately skilled FOCUS IT Analyst is to be selected to conduct an annual check on internal systems for technical security configuration with software based security tools, if applicable; and
— If any internal security configuration results indicated HIGH, MEDIUM or LOW security risks, that a corrective action plan is to be developed and identified security risks mitigated within thirty (30) days.

MONITORING:
- The FOCUS CSO is to review all policies and procedures quarterly to ensure compliance; and
- The FOCUS CSO is to monitor calendar entries to ensure testing is conducted at least annually; and
- The FOCUS CSO is to monitor any findings from security checks until identified risks are mitigated.

EVIDENCE:
- Current policy & procedure; company calendar entries; vendor penetration testing report; internal FOCUS IT Analyst security report; corrective action plans.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Changes to FOCUS information assets, including systems, networks and network services, shall be controlled and archived.0618.09b1System.1 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by creation and maintenance of the **FOCUS change request tracking system,** a feature of the FOCUS Review Management System**,** which must illustrate **the request**, **who made the modifications**, **who tested the change** and **who approved the change**. This system is reviewed annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— All change requests for information assets, systems, networks and network services are entered by requestors into the FOCUS Administration module/IT Inventory System; and
— Approval of all changes must be completed by the CSO; and
— All completed changes are logged into the FOCUS Administration module/IT Inventory System; and
— Automated System IDs and Passwords are to be documented for quick reference within the FOCUS RMS IT module; and
— Automated System IDs are required to meet the FOCUS password policy including composition and change frequency; and
— Automated System IDs are to be stored in encrypted files (The RMS is encrypted and encrypted at rest); and
— Automated System IDs are not to be hard-coded into application(s); and
— Automated System IDs are not to be accessible by end-users.

MONITORING:
- The FOCUS CSO is to review all policies and procedures quarterly to ensure compliance; and
- The FOCUS CSO is to review the FOCUS Administration module/IT Inventory System monthly to review requests and progress of any approved modifications.

EVIDENCE:
- Company calendar entries; FOCUS Administration module/IT Inventory System reports.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS Managers responsible for application systems shall also be responsible for the strict control (change control security) of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment.[0635.10k1Organizational.12] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by creation and maintenance of the **FOCUS change request tracking system,** a feature of the FOCUS Review Management System**,** which must illustrate **the request**, **who made the modifications**, **who tested the change** and **who approved the change**. This system is reviewed annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to change management to determine if managers responsible for application systems are responsible for the security of the project or support environment and ensure that all proposed system changes are reviewed to check that they do not compromise the security of either the system or the operating environment. Further, project and support environments are strictly controlled.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— Appropriately expert FOCUS IT Analysts are trained, attest and comply with this policy, which states they are responsible for the strict control (security) of projects; and
— A risk assessment and analysis of potential impacts must be conducted, documented and approved prior to proceeding; and
— FOCUS IT Analysts are instructed to test all development on test servers to ensure functionality and security before deploying on production servers; and
— FOCUS IT Analysts test to ensure that development does not compromise the security of either the system or the operating environment.

FH internally created the Review Management System, an encapsulated software solution which contains all elements of the system (user interface, tables, logic controls and reporting). This type of system provides a secure environment where programming can be created, tested and activated based on policies regarding alterations or additions to the system. PHI is to be protected at all times, and testing is to be conducted on servers and systems that are not production systems which contain PHI/PII (never on active data). Programming standards to be executed are as follows:

- Each request for additions or changes is documented; and
- The responsible FH Staff developer(s) are assigned; and
- The CEO/CMO and CSO must approve the change(s) before implementation; and
- Changes or additions to the system must be made on the 'test server'; and
- The changes or additions must be thoroughly tested and approved by the CEO/CMO and CSO; and
- The changes or additions are implemented in the production system in low-traffic hours; and
- The changes or additions must be tested in the production system; and
- The log must indicate the history of events before, during and after the implementation.

MONITORING:
- The FOCUS CSO is to review all policies and procedures quarterly to ensure compliance; and
- The FOCUS CSO is to monitor all projects (preparation, in development, in testing, in deployment, deployed).

EVIDENCE:
- Company calendar; training attestations; screen shots of development projects & status.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall manage changes to mobile device operating systems, patch levels, and/or applications through a formal change management process.0671.10k1System.1 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by creation and maintenance of the **FOCUS Administration module/ IT Inventory System,** a feature of the FOCUS Review Management System**,** which must illustrate **the request**, **who made the modifications**, **who tested the change** and **who approved the change**. This system is reviewed annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— Meetings are held and documented with the FOCUS Analyst team members to review device update requirements; and

FOCUS Analyst team members are to:
— Utilize remote management tools to determine if patches are required, applications require updating; and
— Test patches and application updates on non-production test systems prior to installing on systems within the production environment; and
— Utilize remote management tools to install patches and application updates; and
— Document the latest versions of operating systems and applications within the FOCUS Administration module/IT Inventory System; and
— FOCUS IT Analysts are to apply non-critical security patches at least quarterly.

MONITORING:
- The FOCUS CSO is to monitor patch/update activities within the FOCUS Administration module/IT Inventory System.

EVIDENCE:
- Company calendar entries; meeting minutes; FOCUS Administration module/IT Inventory System screenshots.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
Operational systems shall only hold approved programs or executable code.0626.10h1System.3 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by creation and maintenance of the **FOCUS change request tracking system,** a feature of the FOCUS Review Management System**,** which must illustrate **the request**, **who made the modifications**, **who tested the change** and **who approved the change**. Approval of the change must be made by the FOCUS CSO, and a **screenshot illustrating this function** provides evidence. This system is reviewed annually by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
See policy 'Software Development Life Cycle' for additional details.
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— FOCUS IT Analysts remotely control all user systems and servers to ensure that only approved programs or executable code are installed; and
— FOCUS IT Analysts, utilizing the FOCUS Administration module/IT Inventory System must log the current inventory and versions of programs and executable code; and
— Software development is to only be created and tested on designated test servers and is not to be present on production servers.

MONITORING:
- The FOCUS CSO reviews the FOCUS Administration module/IT Inventory System quarterly with emphasis of reviewing the programs and executable code installed on each system or server.

EVIDENCE:
- Company calendar entries; screenshots of remote system management; FOCUS Administration module/IT Inventory System reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain information systems according to a current baseline configuration and configures system security parameters to prevent misuse. Vendor supplied software used in operational systems is maintained at a level supported by the supplier, and uses the latest version of Web browsers on operational systems to take advantage of the latest security functions in the application.0627.10h1System.45 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by **attestations from the CSO and all FOCUS IT Analysis staff members,** and where policy states that **upgrades are prohibited by unauthorized personnel**, which are stored in the FOCUS Review Management System and monitored annually by the CSO. Screenshots of this prohibited activity provides evidence, as well as **screenshots prior to software updates** and **after the update has been installed**. All **patches must be tested** on non-production machine **before being installed on production machines**. **Meeting minutes** must be recorded to this effect. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— FOCUS Administration module/IT Inventory System contains baseline configuration information for each server and workstation for FOCUS IT Analysts to refer and adhere to when configuring systems; and
— All software installed that is acquired by a vendor, installed and operated within specifications of the vendor, on both servers and client workstations, including the most modern supported browser versions to take advantage of the latest security functions in the application.

MONITORING:
- The FOCUS CSO reviews the FOCUS Administration module/IT Inventory System quarterly with emphasis of reviewing baseline configurations documented for each system; and
- Ensure that software installed on servers or workstations are within vendor specifications.

EVIDENCE:
- Company calendar entries; screenshot of FOCUS Administration module/IT Inventory System showing baseline configurations; FOCUS Administration module/IT Inventory System showing vendor specifications and browser requirements.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
If systems or system components in production are no longer supported by the developer, vendor, or manufacturer, FOCUS shall show evidence of a formal migration plan approved by management to replace the system or system components.[0628.10h1System.6] These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by the **FOCUS migration plan, approved by the FOCUS CSO,** which are stored in the FOCUS Review Management System and monitored annually by the CSO. **Meeting minutes** must be recorded to indicate required system modifications and authorization by the CSO. Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
The FOCUS IT Analysts are to:
— Conduct monthly monitoring for all developer, vendor or manufacturers of system components listed within the FOCUS Administration module/IT Inventory System to gain awareness as early as possible when support is scheduled to be discontinued by the source; and
— Identify within the FOCUS Administration module/IT Inventory System any system or system component, on test or production servers, which will or are currently no longer supported by the developer, vendor or manufacturer; and
— Propose to the FOCUS CSO a migration plan to replace the system or system components; and
— The FOCUS CSO creates meeting minutes, documenting details and approval of the migration plan; and
— The FOCUS CSO monitors the FOCUS IT Analyst progress, testing and implementation of the plan until completion.

MONITORING:
- The FOCUS CSO monitors the calendar; and
- The FOCUS IT Analysts monitor all developers, vendors or manufacturers for announced discontinuance of support; and
- The FOCUS CSO monitors all activities regarding strategies of replacement and/or migration and the implementation of replacement components.

EVIDENCE:
- Company calendar entries; screenshot of FOCUS Administration module/IT Inventory System showing system component lists; meeting minutes; migration plans.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 06 CONFIGURATION MANAGEMENT

0601.06g1Organizational.124	HITRUST 06.g Compliance with Security Policies and Standards
0602.06g1Organizational.3	HITRUST 06.g Compliance with Security Policies and Standards
0605.10h1System.12	HITRUST 10.h Control of Operational Software
0663.10h1System.7	HITRUST 10.h Control of Operational Software
0613.06h1Organizational.12	HITRUST 06.h Technical Compliance Checking
0618.09b1System.1	HITRUST 09.b Change Management
0635.10k1Organizational.12	HITRUST 10.k Change Control Procedures
0671.10k1System.1	HITRUST 10.k Change Control Procedures
0626.10h1System.3	HITRUST 10.h Control of Operational Software
0627.10h1System.45	HITRUST 10.h Control of Operational Software
0628.10h1System.6	HITRUST 10.h Control of Operational Software

07 Vulnerability Management

Vulnerability Management Policy

Vulnerability management is a critical component of any security infrastructure because it enables proactive detection and remediation of security vulnerabilities. Security professionals that use vulnerability management tools are able to correct weaknesses before they are exploited and no longer rely solely on defensive security measures to protect themselves.

FOCUS subcontracts independent security vulnerability auditors to analyze our network, systems and policies & procedures to ensure compliance. To this end, FOCUS has established procedures to initiate such audits, review the audit report(s) and institute steps of remediation regarding any outstanding items identified as risks or processes which require actions or corrections to ensure security. FOCUS is to acquire such independent auditing contractors no less than bi-annually (every two years).

FOCUS is to deploy vulnerability detection software, to scan all FOCUS network assets no less than weekly, to automate all steps of the vulnerability management lifecycle process to strengthen the security of the network and conduct automated security audits to ensure compliance with external regulations and internal FOCUS policies.

Vulnerability Management Procedures

FOCUS must acquire (contract) with an independent vulnerability auditing firm for a vulnerability assessment for FOCUS computer networks, systems as well as a review of FOCUS Policies & Procedures no less than annually. The procedures are as follows:

Procedure	Responsibility	Outcome
Identify a qualified, independent vulnerability assessment vendor.	FOCUS CSO	Ensure that the vendor is capable of generating all reports within required time frame.
Contract with the vendor	FOCUS CSO & FOCUS CEO	Contract must stipulate no FOCUS data will be accessed by vendor; deadline must be stipulated.
Submit required data to vendor	FOCUS CSO	Assist vendor with any questions regarding architecture of network infrastructure, IP addresses and policy/procedure documentation for evaluation. At no time may login credentials to FOCUS hardware or software be given to vendor.
Receive & evaluate report(s)	FOCUS CSO	Upon evaluation of the report(s), the CSO must present a summary of the findings to the FOCUS CEO. Any technological inadequacies found must be identified, as well as any Policy/Procedure inadequacies.
Initiate remediation of hardware/ software	FOCUS CSO	Should any technological inadequacies be identified, the CSO must initiate remediation efforts immediately with no more than 30 days to complete all changes to hardware or software.
Initiate remediation of Policies & Procedures	FOCUS CSO & FOCUS CEO	Should any policies & Procedures need modifications to improve security and reduce risks, the FOCUS CSO/CEO must initiate a FOCUS Quality Improvement meeting where changes are proposed and finalized as documented in meeting minutes.
Vendor Follow-Up	FOCUS CSO	Modifications to FOCUS hardware, software and policies & procedures are provided to the vendor. Vendor must re-run the vulnerability analysis in order to confirm that remediation has effectively removed identified risks. A final report must be received from vendor indicating the success or failure of remediation.

Vulnerability Management Testing

The FOCUS CSO is required to ensure that staff training includes the following vulnerability tests, and that an annual inspection must be conducted and documented:

- A test of physical controls for office location(s) (such as a clean desk policy).
- Testing of the process for obtaining system access to ensure the proper steps are followed.
- Testing to ensure system accesses are reviewed for appropriateness.
- Testing of the prompt removal of system access when an employee separates from the company.

Note: This security document outlines policies & procedures regarding several of the items listed above.
Testing further confirms that the policies & procedures herein are being followed appropriately.

Application Security Standards

While the FH Review Management System is a self contained singular system, safeguards are to be maintained to minimize exposure of any and all data within the RMS. These safeguards include:

- Automatic discontinuance (log-out) of the system after one (1) hour of inactivity on the part of any user; and
- Regular, automated and mandatory (at least monthly) changing of passwords by all users; and
- Discontinuance of any user that has departed a client-company, FH staff or FH peer reviewers; and
- FH policy stating that users not record and/or distribute any FH data to any company or person outside of FH staff members, FH peer reviewers or FH client-companies.
- Automated discontinuance of access by any user after 30 days, for all system users.

POLICY:
FOCUS shall provide for data confidentiality and security of its information system(s) (*electronic* and paper) by implementing written policies and/or documented procedures that address C-15 : (No Weight)

(a) Assessment of the potential risks and vulnerabilities to the confidentiality, integrity and availability of information systems; (3)
(b) Prevention of confidentiality and security breaches; **and** (Mandatory)
(c) Detection, containment and correction of confidentiality and security violations. (Mandatory)

This URAC standard is embodied in the FOCUS Information Protection Program. Policies and procedures for the management of required elements include the **FOCUS Risk Assessment Policy and Procedure**(a); and the **FOCUS Security Policy and Procedure**(b),(c). Measurement of success is abased on the creation, maintenance, and accurate execution of these FOCUS Policies and procedures; assessing risks; preventing breaches and managing security violations. Evidence shall include performing annual assessments of risks and vulnerabilities, initial training and annual training (with attestations) of FOCUS staff members and Peer Reviewers; and providing a **PHI reporting mechanism** within the FOCUS Review Management System for all stakeholders to report suspected or actual breaches of PHI. Ongoing quality assurance monitoring mechanisms include an annual review of the programs, policies and procedures, and ongoing monitoring of reports and logs with quarterly meetings documented in meeting minutes. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
— The FOCUS CSO ensures that calendar entries are made for reviewing this policy annually; and
— Please refer to the FOCUS Risk Assessment Policy and Procedure; and
— PHI Reporting Mechanism, served within the FOCUS Review Management System; and
— Prevent confidentiality and security breaches by reviewing and ensuring that all applicable policies & procedures are followed by all FOCUS staff and Peer Reviewers; and

The FOCUS CSO is to:
— Ensure initial training for all new staff members (and annually, thereafter) of all FOCUS policies; and
— Ensure annual review of the aforementioned policies and PHI Reporting Mechanism; and
— Monitor for the detection, containment and correction of confidentiality and security violations; and
— Document quarterly meeting minutes to review/update the PHI Reporting Mechanism.

MONITORING:
The FOCUS CSO is to:
• Monitor the company calendar entries requiring annual policy review and annual risk assessments; and
• Review, on an annual basis, all security related policies & procedures; and
• Review, on a quarterly basis, all training logs and ensure that attendees read, understand, attest and comply; and
• Monitor the PHI Reporting Mechanism for possible security violations and conduct documented meetings, as necessary.

EVIDENCE:
• Company calendar entries; risk assessments; all security-related policies & procedures; meeting minutes; training attestations.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
An inventory of FOCUS assets and services shall be maintained.0701.07a1Organizational.12 These requirements are stipulated in the **FOCUS Security Policy and Procedure**. Measurement of success for this FOCUS policy is based on evidence collected by the **screenshots** of the **FOCUS RMS Administrative module/IT Inventory System** and **Reports** generated by this system**.** Ongoing quality assurance monitoring mechanisms include monitoring of evidence quarterly by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar. The FOCUS CSO and IT Analysts must confirm that the inventory for each asset includes information on type or classification of the asset, format, location, backup information, license information, business value, encryption and portable/personal device, and the FH inventory system shall have checks and/or safeuards to prevent duplicates. Asset Management is composed of four categories:

Accountability and Inventory
FH is dedicated to tracking and accurately managing asset inventories. This is to clarify ownership of assets and define stewardship of assets for the company. Utilizing the RMS Administration Module, the CSO shall inventory all technological assets of the company, and identify which assets are assigned to each individual employee or data center location. Value of the asset is assessed, and criticality of the asset regarding its' role in the business is specified.

Classification
The FH Chief Security Officer shall classify assets based on business impact, including the potential of privacy violations, if applicable. Classification categories are applied to each item in the inventory system. Classification categories include (but are not limited to): (1) Confidential; (2) Sensitive; (3) Public.

Labeling
Standards of labeling assets clearly state their classification, and identification numbering clearly links the asset to the inventory database.

Handling
Providing a FH staff member (introduction), as well as transfers, removal and disposal of all assets must be documented in the asset inventory system.

FOCUS shall examine policies and/or standards related to the inventory of assets and services to determine if the organization identifies and inventories all assets including information (e.g., PII), encrypted or unencrypted, wherever it is created, received, maintained, or transmitted, including organizational and third-party sites, and document the importance of these assets.

Deliverable Assets
As for reports and on-screen user interface graphics, a clear indicator of client-company names shall be clearly visible so that these assets are identifiable when viewed and/or transmitted to client companies.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— The FOCUS RMS Administrative module/IT Inventory System includes a comprehensive asset and systems inventory tracking mechanism; and
— Access to this system includes the FOCUS CSO and FOCUS Analysts to add/modify to the inventory and include a wide variety of specific data regarding systems and services.
— The FOCUS CSO and IT Analysts must maintain the inventory data by navigating within the FOCUS RMS Administration module to:
RMS » ADMIN » IT » IT ASSETS » DATA CENTER COMPUTERS; and
RMS » ADMIN » IT » IT ASSETS » END USER COMPUTERS; and
RMS » ADMIN » IT » IT ASSETS » NETWORK DEVICES; and
RMS » ADMIN » IT » IT ASSETS » SOFTWARE LICENSES; and
RMS » ADMIN » IT » IT ASSETS » LEASES
— The FOCUS CSO and IT Analysts are to confirm that the inventory for each asset includes information on type or classification of the asset, format, location, backup information, license information, business value, encryption and portable/personal device.

MONITORING:
- The FOCUS CSO monitors the FOCUS RMS Administrative module/IT Inventory System at least quarterly to maintain familiarity with all inventory assets and services; and
- The FOCUS IT Analysts monitor the FOCUS RMS Administrative module/IT Inventory System for content accuracy.

EVIDENCE:

• Company calendar; screen shots of FOCUS RMS Administrative module/IT Inventory System.

RESPONSIBLE PARTY:

• FOCUS IT Analyst

POLICY:

The information lifecycle shall manage the secure use, transfer, exchange, and disposal of FOCUS IT-related assets. 0702.07a1Organizational.3 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on evidence collected by the instructions to FOCUS IT Staff within the policy; a function within the FOCUS Review Management System to **track and manage assets**; **Reports** generated by this function**;** and quarterly **monitoring and review of IT activities** related to asset management by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar. The FOCUS CSO is responsible to determine the best disposal method for destroyed hard drives.

PROCEDURES:

The FOCUS CSO ensures that:

— Calendar entries are made for reviewing this policy annually; and

— The FOCUS RMS Administrative module/IT Inventory System is to include a comprehensive asset and systems inventory tracking mechanism which clearly indicates, per IT asset, the history of secure use, transfer, exchange, and disposal; and

— Access to this system includes the FOCUS CSO and FOCUS Analysts to add/modify to the inventory to transfer, exchange and dispose of equipment as necessary, with approval documented by the FOCUS CSO within this system; and

— Disposal of hard drives are to be conducted by physically drilling through the drive at least 5 (five) times and delivered to a toxic waste disposal facility; and

— The FOCUS CSO and FOCUS IT Analysts are to document use, transfer, exchange and disposal within the RMS Admin Module at: RMS » ADMIN » IT » IT ASSETS » COMPUTERS

— The FOCUS IT Staff Member who destroys any IT asset is to attest to the destruction and disposal in the RMS.

— The FOCUS CSO has determined the best disposal method for destroyed hard drives. The FOCUS CSO ensures that the FOCUS IT Analysts dispose of hard drives by this method. The FOCUS CSO has concluded that approved disposal is as follows:

  • After physical destruction of the hard disk drive, the FOCUS IT Analyst are to deliver the destroyed drive to:

  • Hernando County, Florida 'Transfer Station' for Solid Waste Disposal facility
  2525 Osowaw Blvd., Spring Hill, FL 34607 - Ph: 352-754-4770
  URL: https://www.hernandocounty.us/departments/departments-n-z/solid-waste-and-recycling/solid-waste-facilities-drop-off-information

MONITORING:

• The FOCUS CSO monitors the FOCUS RMS Administrative module/IT Inventory System at least quarterly to maintain familiarity with all items and the status of inventory; and

• The FOCUS Analysts monitor the FOCUS RMS Administrative module/IT Inventory System for content accuracy.

EVIDENCE:

• Company calendar; screen shots of FOCUS RMS Administrative module/IT Inventory System.

PRIMARY RESPONSIBLE PARTY:

• FOCUS CSO

SECONDARY RESPONSIBLE PARTIE(S)

• FOCUS IT Analysts

POLICY:
Applications developed by FOCUS shall be based on secure coding guidelines to prevent common vulnerabilities or undergo appropriate testing. 0706.10b1System.12 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** to include **coding guidelines** reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on evidence collected by a **software add/change request function** within the FOCUS Review Management System for tracking the creation or modification of the FOCUS Review Management System; adherence by FOCUS IT staff members to the FOCUS Security Policy and Procedure regarding **new/modified software testing** prior to entering production**;** approval of tested software by the FOCUS CSO before and quarterly **monitoring and review of IT activities** related to development by the CSO. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— Please refer to FOCUS policy entitled 'OWASP T10 Security Policy.pdf' for details regarding software development security requirements; and
— FOCUS IT Analysts with job descriptions which include internal software development are provided training and are provided materials and policies reflecting secure coding guidelines and must read/understand/attest and comply with all FOCUS procedures regarding software security and testing prior to deployment.

MONITORING:
- The FOCUS CSO monitors training and ensure that FOCUS IT Analysts that develop software have attested to all policies.

EVIDENCE:
- Company calendar; screen shots of FOCUS RMS Administrative module/IT Inventory System.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS Technical vulnerabilities shall be identified, evaluated for risk and corrected in a timely manner. 0709.10m1Organizational.1 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** and the **FOCUS Business Continuity Policy and Procedure**; both reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on evidence collected by an **independent vulnerability scan.** Review of the independent vulnerability scan report and **completion of all corrective actions**, by the FOCUS CSO within 60 days or less. Further, quarterly activities of **monitoring and review of any suspected or actual vulnerabilities** between scans is to be documented by the CSO in **meeting minutes.** All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to technical vulnerability management and determine if once a potential technical vulnerability has been identified, the organization identifies the associated risks and the actions to be taken. Such action involves patching of vulnerable systems and/or applying other controls.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— At least annually an external scan of all IP's in use are to be conducted by an independent penetration organization; and
— The results of mentioned scan will be reviewed and any remediation done before a secondary scan performed to show clearance of any items identified.
— In the event internal technical vulnerabilities are identified, the FOCUS CSO is to hold documented meetings with FOCUS IT Analysts to discuss remediation steps and monitor remediations until completed. Critical findings must be remediated within 48 hours.

MONITORING:
- The FOCUS CSO reviews the results of the independent penetration scan and oversee any remediation needed; and
- The FOCUS CSO is to ensure the remediation is complete and a second scan is performed showing compliance.

EVIDENCE:
- Company calendar; meeting minutes; completed independent vendor specialist penetration scan.

POLICY:
FOCUS's asset inventory shall not duplicate other inventories unnecessarily and ensures their respective content is aligned. 0720.07a1Organizational.4 These requirements are stipulated in the **FOCUS Security Policy and Procedure** which is reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on evidence by **reports generated** by the FOCUS Review Management System from the **IT inventory function** with oversight by the FOCUS CSO. Quarterly activities of **monitoring of inventory reports** is to be documented by the CSO in **meeting minutes**. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— The FOCUS RMS Administrative module/IT Inventory System is to provide a relational database to provide a centralized storage warehouse of information for all stakeholders to access, which prevents duplicate lists (such as individual spreadsheets); and
— Access to this system includes the FOCUS CSO and FOCUS Analysts to add/modify to the inventory and include a wide variety of specific data regarding systems and services.

MONITORING:
- The FOCUS CSO monitors the FOCUS RMS Administrative module/IT Inventory System at least quarterly to maintain familiarity with all items and the status of services; and
- The FOCUS Analysts are to monitor the FOCUS RMS Administrative module/IT Inventory System for content accuracy.

EVIDENCE:
- Company calendar; screen shots of FOCUS RMS Administrative module/IT Inventory System.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain an inventory of authorized wireless access points, including a documented business justification to support unauthorized WAP identification and response. 0721.07a1Organizational.5 These requirements are stipulated in the **FOCUS Security Policy and Procedure** which is reviewed and approved annually by FOCUS management. This is provided in FOCUS staff member **training** (**with attestations**) and reiterated/documented within IT **meeting minutes**. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that wireless access points are prohibited.

PROCEDURES:
— It is FOCUS policy that wireless access points are prohibited as of the date of this policy effective date; and
— In the event FOCUS modifies this prohibition, this policy will be update to address the HITRUST requirement in full.

MONITORING:
- No monitoring currently required.

EVIDENCE:
- No evidence currently required.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
If FOCUS assigns assets to contractors, it shall ensure that the procedures for assigning and monitoring the use of the property are included in the contract; and, if assigned to volunteer workers, there is a written agreement specifying how and when the property will be inventoried and how it will be returned upon completion of the volunteer assignment. 0722.07a1Organizational.67 These requirements are stipulated in the **FOCUS Security Policy and Procedure** which is reviewed and approved annually by FOCUS management. This is provided in FOCUS contractor (Peer Reviewer) training and reiterated/documented within IT **meeting minutes**. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS that contractors are prohibited from receiving any FOCUS assets**.**

PROCEDURES:
— It is the policy of FOCUS that contractors are prohibited from receiving any FOCUS assets as of the date of this policy effective date; and
— In the event FOCUS modifies this prohibition, this policy will be update to address the HITRUST requirement in full.

MONITORING:
- No monitoring currently required.

EVIDENCE:
- No evidence currently required.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall create and document the process/procedure FOCUS intends to use for deleting data from hard-drives prior to property transfer, exchange, or disposal/surplus. 0723.07a1Organizational.8 These requirements are stipulated in the **FOCUS Security Policy and Procedure** which is reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on the **procedural instructions within the 'Information Technology' policy.** Further evidence shall include a **screenshot demonstrating 'remote wipe' capabilities**. This is provided in FOCUS IT staff member **training** (**with attestations**) and reiterated/ documented within IT **meeting minutes**. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
— Calendar entries are made for reviewing this policy annually; and
— Please refer to the FOCUS policy entitled 'Information Technology.pdf' for detailed procedures regarding the creation and documentation the process/procedure to be used for deleting data from hard-drives prior to property transfer, exchange, or disposal/ surplus.

MONITORING:
- The FOCUS CSO is to review this policy annually; and

EVIDENCE:
- Company calendar entries; screenshot of remote wipe capabilities; historical photographic evidence of destroyed hard drives.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS applications that store, process or transmit covered information shall undergo automated application vulnerability testing by a qualified party on an annual basis. 0707.10b2System.1 These requirements are stipulated in the **FOCUS Security Policy and Procedure** which is reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on the **procedural instructions within the security policy.** Further evidence shall include a **security best practices audit report**. This is provided in FOCUS IT staff member **training** (**with attestations**) and reiterated/documented within IT **meeting minutes**. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to input validation in applications to determine if applications which store, process or transmit covered information undergo automated (non-manual) application vulnerability testing with an emphasis on input validation controls at least annually by a qualified party.

NOTE: FOCUS has acquired a commercial software package that is a compiled program. FOCUS Analysts develop no code.

PROCEDURES:
The FOCUS CSO ensures that:
— Calendar entries are made for reviewing this policy annually; and
— A qualified FOCUS IT Analyst is to access the following tools to assess vulnerability of the FOCUS RMS:
  • FileMaker 19 Security Guide: Best Practices; and
  • FOCUS policy entitled 'OWASP T10 Security Policy v 6.0.pdf'; and
  • FOCUS Software Development Lifecycle
— FOCUS utilizes a commercial application (FileMaker) to build the RMS, which does not provide a development environment with risk-prone code-level development; therefore there are no automated application vulnerability testing tools. However, the FOCUS CSO and IT Analysts are to conduct research on a quarterly basis in an effort to find such an automated tool; and
— The qualified FOCUS IT Analyst, using the FileMaker security best practices guide, creates a 'security best practices audit report' illustrating that all best practices are confirmed to be active; and
— The FOCUS CSO reviews each quarterly 'security best practices audit report' and if required, develop a corrective action plan; and
— The upon hiring an independent penetration testing vendor, the FOCUS CSO requires that an application penetration test be conducted during each regular network penetration testing cycle.

MONITORING:
  • The FOCUS CSO reviews this policy annually; and
  • The FOCUS CSO monitors calendar entries for annual and quarterly required processes; and
  • The FOCUS CSO reviews each quarterly 'security best practices audit report' and document the results in meeting minutes with the IT Analyst(s).

EVIDENCE:
  • Company calendar entries; meeting minutes; 'security best practices audit report'.

RESPONSIBLE PARTY:
  • FOCUS IT Analyst

POLICY:
FOCUS system and information integrity requirements shall be developed, documented, disseminated, reviewed and updated annually. 0708.10b2System.2 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** that refers to the **FOCUS 'Information Technology'** policy and **'System and Information Integrity'** policy**,** which is reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on the section entitled **information integrity requirements** within the **'System and Information Integrity'** policy**;** and **'Information Technology'** policy**.** This is provided in FOCUS staff member end-user **training** (**with attestations**) and client-company end user training. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to system and information integrity to determine if the organization: (i) develops and documents system and information integrity policy and procedures;
(ii) disseminates the system and information integrity policy and procedures to appropriate areas within the organization; and, (iii) reviews and updates defined system and information integrity requirements no less than annually.

NOTE: FOCUS has acquired a commercial software package that is a compiled program. FOCUS Analysts develop no code.

PROCEDURES:
— Please refer to FOCUS Policy entitled 'Information Technology v 12.0.pdf'; and
— Please refer to FOCUS Policy entitled 'System and Information Integrity v1.0.pdf';and
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is provided to FOCUS IT Analysts to ensure understanding/attestation/compliance with the policies.

MONITORING:
- The FOCUS CSO monitors the company calendar for policy review dates; and
- The FOCUS CSO monitors training events and ensure appropriate staff understand and attest to policies; and
- The FOCUS CSO, using the FOCUS RMS Administrative module/IT Inventory System to review all FOCUS information systems meet or exceed the above policy requirements.

EVIDENCE:
- Company calendar; active policies; training attestations; screenshots of FOCUS RMS Administrative module/IT Inventory System regarding information integrity documentation.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The information system checks the validity of organization-defined information inputs for accuracy, completeness, validity, and authenticity as close to the point of origin as possible. For in-house developed software, FOCUS ensures that explicit error checking is performed and documented for all input, including for size, data type, and acceptable ranges or formats. 0733.10b2System.4 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** that includes **coding guidelines,** and **data entry validation rules,** which is reviewed and approved annually by FOCUS management. Measurement of success for this FOCUS policy is based on the section entitled **information integrity requirements** within the **security policy;** and the **FOCUS CSO shall review and confirm validation and error checking routines** on a quarterly basis**.** This is provided in FOCUS staff member end-user **training** (**with attestations**) and client-company end user training. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: FOCUS has acquired a commercial software package that is a compiled program. FOCUS Analysts develop no code.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A confirmatory review of the integrated input validation and error checking rules to ensure compliance on a quarterly basis, documented in meeting minutes with the FOCUS IT Analysts.
FOCUS IT Analysts are to:
— Install automated input validation (e.g. date/time format accuracy, input from predetermined options only, etc.) for accuracy, completeness and authenticity (via the FOCUS RMS audit log); and
— Install automated error checking for all input (including for size, data type, and acceptable ranges or formats).

MONITORING:
- The FOCUS CSO monitors for policy review calendar events; and
- The FOCUS CSO monitors the FOCUS IT Analyst implementation of validation and error checking solutions.

EVIDENCE:
- Company calendar; active policies; RMS audit log report; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Procedures, guidelines, and standards for the development of applications are periodically reviewed, assessed and updated as necessary by the appointed senior-level information security official of FOCUS. 0791.10b2Organizational.4 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** that includes **coding guidelines,** which is reviewed and approved annually by FOCUS management. Annual reviews of this segment of the FOCUS Security Policy and Procedure will be documented in meeting minutes. The FOCUS CSO shall review all active policies quarterly with the FOCUS IT Analyst team members. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: FOCUS has acquired a commercial software package that is a compiled program. FOCUS Analysts develop no code.

PROCEDURES:
— Please refer to FOCUS Policy entitled 'Information Technology v 12.0.pdf'; and
— Please refer to FOCUS Policy entitled 'System and Information Integrity v1.0.pdf'; and
— OWASP T10 Security Policy v 6.0.pdf; and
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO reviews procedures, guidelines, and standards for the development of applications on an annual basis.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO monitors utilization of these policies by the FOCUS IT Analysts quarterly.

EVIDENCE:
- Company calendar; active policies; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS

URAC C15	*URAC IRO CORE 15: Information Confidentiality and Security*
0701.07a1Organizational.12	HITRUST 07.a Inventory of Assets
0702.07a1Organizational.3	HITRUST 07.a Inventory of Assets
0706.10b1System.12	HITRUST 10.b Input Data Validation
0709.10m1Organizational.1	HITRUST 10.m Control of Technical Vulnerabilities
0720.07a1Organizational.4	HITRUST 07.a Inventory of Assets
0721.07a1Organizational.5	HITRUST 07.a Inventory of Assets
0722.07a1Organizational.67	HITRUST 07.a Inventory of Assets
0723.07a1Organizational.8	HITRUST 07.a Inventory of Assets
0707.10b2System.1	HITRUST 10.b Input Data Validation
0708.10b2System.2	HITRUST 10.b Input Data Validation
0733.10b2System.4	HITRUST 10.b Input Data Validation
0791.10b2Organizational.4	HITRUST 10.b Input Data Validation

NETWORK AND SYSTEMS SECURITY

Network security deals with concerns about the integrity and confidentiality of data traversing the network as well as the potential for security incidents (denial of service, unauthorized access, etc.) that occur over the network.

Computer System Security

There are two types of computing security on which FH has focused. These are:

1) Operating system security; and
2) User data security (Accessed via the FH Review Management System)

While these two types may be seen as having distinct boundaries between the users' and FH staff's responsibilities, both FH and its user communities must work together to ensure a secure environment for all.

The operating system security goals are fivefold:

1) To prevent access to the systems by unauthorized users; and
2) To prevent users with valid logins from unauthorized data access; and
3) To prevent unauthorized use of computing resources; and
4) To maintain system availability; and
5) To prevent errors by those authorized to make system level changes.

The security for the operating system environment is shared by FH and the end users (FH staff members and FH peer reviewers). Security for the operating system of FH client-companies are with their respective Information Technology departments.

FH staff members of all machines are required to keep their machines up to date with the most current patches to the operating systems. All unnecessary services should be disabled. System scans may be performed by the FH Information Technology staff members for vulnerabilities on all machines, and administrators may be notified to install specific patches to address vulnerabilities.

While FH staff members utilize Apple Macintosh computers exclusively, FH peer reviewers running Windows machines are required to install and run an FH approved anti-virus package. These also need to be kept updated according to the vendor’s recommendations.

If a machine appears to have been compromised, access to the FH Review Management System may be revoked by the authority of the FH Security Officer.

If you feel your electronic workplace (e.g., your account, or machine you utilize) is compromised, or if you observe suspicious electronic behavior you are not sure about, immediately cease access to the FH Review Management System and contact the FH Security Officer, which can be reached at 727-647-8023. Alternatively, call the FH technical support number of 866-561-9542 for immediate assistance. Users are encouraged to make every effort to secure their own data.

POLICY:
FOCUS's security gateways (e.g. firewalls) shall enforce security policies and are configured to filter traffic between domains, block unauthorized access, and are used to maintain segregation between internal wired, internal wireless, and external network segments (e.g., the Internet) including DMZs and enforce access control policies for each of the domains. *0805.01m1Organizational.12* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be in the form of **screenshots** of the ASA configuration and **ASA system reports**. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to network segregation and determine if security gateways (e.g., a firewall) is used between the internal network, external networks (Internet and third-party networks), and any demilitarized zone (DMZ). An internal network perimeter is implemented by installing a secure gateway (e.g., a firewall) between two interconnected networks to control access and information flow between the two domains. This gateway is capable of enforcing security policies, be configured to filter traffic between these domains, and block unauthorized access in accordance with the organization's access control policy. Wireless networks are segregated from internal and private networks. The organization requires a firewall between any wireless network and the covered information systems environment.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
The FOCUS IT Analysts ensures that:
— The Security Appliance (Cisco ASA) is to be configured:
- For traffic filtering: Ensure the rules on the ASA (firewall) by default denies all and is open for the ports necessary to the IP authorized.
- For blocking unauthorized access: Blocking of all traffic but which was authorized by FOCUS CSO.
- Regarding segregation between internal wired, wireless and external network segments: FOCUS does not have any wireless access and no external network segments. All traffic from external to internal and vice-versa is controlled by the ASA (firewall).

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The FOCUS CSO holds documented quarterly meetings to confirm ASA configuration appropriateness.

EVIDENCE:
- Company calendar; screenshots of the ASA configuration; ASA system reports; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
The ability of users to connect to the internal network shall be restricted using a deny-by-default and allow-by-exception policy at managed interfaces according to the access control policy and the requirements of clinical and business applications. *0814.01n1Organizational.12*
These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be in the form of **screenshots** of the ASA configuration, **screenshots** illustrating denial-by-default by the ASA, and **FOCUS RMS screenshots** illustrating denial of access. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
The FOCUS IT Analysts must:
— Configure the ASA to 'deny-by-default and allow-by-exception; and
— Ensure that screenshots of configuration are stored in the RMS; and
— Ensure that screenshots of denial-by-default and allow-by-exception are stored in the RMS.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO ensures that the FOCUS IT Analyst, by documented meeting minutes, has confirmed and collected evidence to demonstrate security appliance (firewall) configuration as stipulated by this policy.

EVIDENCE:
- Company calendar; screenshots of FBH denial; screenshots of ASA denial; screenshots of ASA configuration.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:

The sensitivity of FOCUS applications/systems shall be explicitly identified and documented by the application/system owner. *0816.01w1System.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that the supporting document is current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

The FOCUS CSO evaluates all systems to determine which systems provide access to, process, report and contain Personal Health Information (PHI) and/or Personally Identifiable Information (PII). As of this version of the FOCUS Security Policy & Procedure, FOCUS has a singular system (known as a 'sensitive system') which is hosted on a dedicated server computer, contains both PHI and PII, known as the FOCUS Review Management System (RMS). This system is a centralized repository of data (DB) which also provides a user interface (UI) so that stakeholders may access the system after providing proper credentials. This system provides customized versions of FOCUS' Privacy Policy and Terms of Service to each stakeholder category, which provides detailed descriptions, requirements of the user, contact information, and other critical elements to ensure security of the PHI/PII. So as to maintain all PHI/PII within the FOCUS RMS, all other methods of collecting, distributing, sharing, storing, photographing, copying, notating and screenshots of PHI/PII is prohibited (e.g., emailing, storing on external disks, thumb drives, photographing, handwriting notes, screenshots).

PROCEDURES:

The FOCUS CSO ensures that:

— These policies are reviewed/modified/ratified no less than annually; and

— Within the FOCUS RMS Administration module/IT Inventory system, documentation regarding each FOCUS application (e.g., the RMS), is to have explicitly identified and documented information regarding the sensitivity of applications/systems so that FOCUS IT Analysts may refer to this information and clearly know which systems contain sensitive information; and

— Hold documented meetings and confirm on a quarterly basis that information regarding sensitive systems/applications is current.

— In the event any additional 'sensitive system' beyond the use of the FOCUS RMS were to be utilized for any PHI/PII processing, the FOCUS CSO is to immediately update all effected areas of this policy and ensure that documentation, development, training, vendor agreements and all other necessary steps are taken to properly activate any additional sensitive system(s) prior to use.

MONITORING:

- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO ensures accurate/current information regarding which systems manage sensitive information.

EVIDENCE

- Company calendar; screenshot of FOCUS RMS Administration module/IT Inventory system illustrating sensitive system documentation; meeting minutes.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain a current network diagram (including wireless networks) and is updated whenever there are network changes and no less than every six months. *0819.09m1Organizational.23* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FOCUS Network Diagram'**. Evidence shall be in a **supporting document** stored in the FOCUS Review Management System entitled 'FOCUS Network Diagram'. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a semi-annual basis to ensure that the supporting document is current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the management of the network and determine if a current network diagram exists documenting all high-risk environments, data flows, and connections to systems storing, processing or transmitting covered information, including any wireless networks that may have legal compliance impacts. The network diagram is updated based on changes to the network, or is updated no less than every six months.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— See 'FOCUS Network Diagram' for illustrated network within the FOCUS Data Center; and
— Hold a documented meeting with FOCUS IT Analysts quarterly to ensure that the network diagram is updated in a timely manner; and
The FOCUS IT Analysts:
— Maintain a modernized version and historical inventory of the FOCUS Network Diagram and store it with the FOCUS RMS Administration System/Supporting Documents section.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance and periodic network diagram updates; and
- The CSO ensures that the network diagram has been updated and is on file.

EVIDENCE:
- Company calendar, FOCUS network diagram, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
Agreed services provided by a network service provider/manager to FOCUS shall be formally managed and monitored to ensure they are provided securely. *0835.09n1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is the policy that FOCUS manages the network utilizing FOCUS employees only. In the event FOCUS modifies this policy and allows third party organizations to work on the FOCUS network in the future, this policy shall be updated to include all required processes ensuring security, stability and proper documentation by the third party. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that the supporting document is current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the management of network services and determine if the ability of the network service provider to manage agreed services in a secure way is determined and regularly monitored, and the right to audit is agreed by management. The security arrangements necessary for particular services including security features, service levels, and management requirements, is identified and documented.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— At the time of this policy effective date, it is the policy that FOCUS manages the network utilizing FOCUS employees only; and
— In the event FOCUS modifies this policy and allows third party organizations to work on the FOCUS network in the future, this policy is to be updated to include all required processes ensuring security, stability and proper documentation by the third party.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance.

EVIDENCE:
- Company calendar entries; effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
Routing controls shall be implemented through FOCUS' security gateways (e.g., firewalls) used between internal and external networks (e.g., the Internet and 3rd party networks). *0850.01o1Organizational.12* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Routing Controls'**. Per Policy, routing controls shall **require Virtual Private Network** (VPN) access. Further evidence shall be the **documented firewall rules**, stored in the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that the firewall rules are documented and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented meeting is held quarterly to review and ensure that the Security Appliance routing controls are implemented through firewalls between internal and external networks.
The FOCUS IT Analysts ensure that:
— The Security Appliance (Cisco ASA) configuration routing controls are to be documented within the RMS location of RMS -> IT -> INVENTORY -> ASA

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The FOCUS IT Analysts ensures that the Security Appliance is configured on a quarterly basis.

EVIDENCE:
- Company calendar entries; screenshots of ASA configurations; effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure the security of information in networks, availability of network services and information services using the network, and the protection of connected services from unauthorized access. *0859.09m1Organizational.78* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Routing Controls'**. Per Policy, routing controls shall **require Virtual Private Network** (VPN) access. Further evidence shall be the **documented firewall rules, firewall logs**, and the FOCUS RMS Server log (to track unsuccessful attempts) and the FOCUS RMS login report (to track successful attempts) which shall be stored in the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all reports and logs are documented and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
— Please refer to FOCUS Policy entitled 'Information Technology v 12.0.pdf'; and
— Please refer to FOCUS Policy entitled 'System and Information Integrity v1.0.pdf'; and
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented meeting is held quarterly to ensure that all reports and logs are documented and accurate; and
The FOCUS IT Analysts ensure that:
— VPN (Virtual Private Network) must be active and required to access FOCUS systems internally, illustrated by screenshot of Security Appliance configuration; and
— Automated notifications are functional to alert the FOCUS CSO and FOCUS IT Analysts in the event of an outage to ensure constant availability; and
— Protection of connected services, such as SSL certificate specifications/files/data are active and functional; and
— VPN configuration, Automated Notifications and Protection of connected services, have been configured and documented within the FOCUS RMS Administrative module/IT Inventory system.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The FOCUS IT Analysts ensures that the Security Appliance and other services required to fulfill this policy is configured and documented for review on a quarterly basis.

EVIDENCE:
- Company calendar entries; screenshots of ASA configurations; screenshots of SSL configurations, effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall monitor for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAPs) unless explicitly authorized in writing by the CSO or his/her designated representative. *0858.09m1Organizational.4*
These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. An annual review of this policy shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS to not have any wireless access points on the FOCUS network.

PROCEDURES:
— It is the policy of FOCUS to not have any wireless access points on the FOCUS network.
— In the event this policy changes to allow wireless access points, the FOCUS CSO updates this policy to define monitoring for all authorized and unauthorized wireless access to the information system and prohibits installation of wireless access points (WAPs) unless explicitly authorized in writing by the CSO or his/her designated representative.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance.

EVIDENCE:
- Company calendar entries; effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall formally manage equipment on the network, including equipment in user areas. *0860.09m1Organizational.9* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Network Equipment'**. Evidence shall be the written policy; **remote management tool** screenshots; **access control** screenshots of client remote access software (Remote Desktop); Screenshot of **ASA administrative screen**; and screenshot of **ethernet switch management** software, which shall be stored in the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all screenshots are documented and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented quarterly review meeting to ensure that the FOCUS RMS Administration module/IT Inventory System is accurate; and
The FOCUS IT Analysts ensures that:
— All FOCUS networking equipment in the data center is formally managed by only allowing the FOCUS CSO or FOCUS IT Analysts access to the FOCUS cabinet data center and will document management of these systems in the FOCUS RMS Administration module/IT Inventory System; and
— All FOCUS equipment in remote locations is formally managed by only allowing the FOCUS CSO or FOCUS IT Analysts access to these systems for configuration and will document management of these systems in the FOCUS RMS Administration module/IT Inventory System; and

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO monitors the FOCUS RMS Administration module/IT Inventory System.

EVIDENCE:
- Company calendar entries; effective policy; FOCUS RMS Administration module/IT Inventory System network configuration screenshots.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
For any public-facing FOCUS Web applications, FOCUS shall ensure that application-level firewalls have been implemented to control traffic. For any public-facing applications that are not Web-based, FOCUS has implemented a network-based firewall specific to the application type. If the traffic to the public-facing application is encrypted, ensuring that the device either sits behind the encryption or is capable of decrypting the traffic prior to analysis. *0808.10b2System.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Routing Controls'**. Evidence shall be the written policy; **firewall rules** screenshots; **encryption** of port 443 and nationally signed SSL certificate(s). Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all certificates and screenshots are documented and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the prevention of Web-based attacks to determine if for public-facing Web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods (i) reviewing applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes; and, (ii) installing an automated technical solution that detects and prevents Web-based attacks (e.g., Web-application firewalls) are placed in front of public-facing Web applications to continually check all traffic. If a public-facing application is not Web-based, the organization implements a network-based firewall specific to the application type. If the traffic to the public-facing application is encrypted, the device should either sit behind the encryption or be capable of decrypting the traffic prior to analysis.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented quarterly review meeting with FOCUS IT Analysts is held to ensure that public-facing web applications and application-level firewalls are implemented; and
The FOCUS IT Analysts ensures that:
— Utilizing the ASA configuration screen, public-facing web applications are to be traffic-controlled to ensure isolation from the internal FOCUS local area network; and
— Firewalls within the FOCUS RMS application have been implemented to control traffic as well.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO conducts a quarterly meeting with FOCUS IT Analysts to document monitoring activities.

EVIDENCE:
- Company calendar entries; quarterly meeting minutes; effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
The FOCUS network shall be logically and physically segmented with a defined security perimeter and a graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network, based on organizational requirements; and traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements. *0806.01m2Organizational.12356* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Routing Controls**'. Evidence shall be the written policy; **firewall rules** screenshots; a supporting document entitled **'FOCUS LAN configuration'** and **'FOCUS Review Management System Architecture'**. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all evidence and supporting documents are up-to-date and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold documented quarterly meetings with FOCUS IT Analysts to review and ensure that network configuration meets this policy; and
— Risk assessments for the RMS are documented in the FOCUS RMS Administration module/IT Inventory System for FOCUS IT Analysts to access and consider when configuring the network; and
The FOCUS IT Analysts:
— Ensure that the FOCUS network is logically and physically segmented with a defined security perimeter and graduated set of controls, including subnetworks for publicly accessible system components that are logically separated from the internal network, based on organizational requirements by implementation of a singular network segment, as FOCUS is a virtual company and has no inventory of disparate locations to interconnect. All stakeholders (users) must connect from individually remote locations to the FOCUS data center.
— Ensure that traffic is controlled based on functionality required and classification of the data/systems based on a risk assessment and their respective security requirements by the implementation of pre-categorized user privilege sets, which imposes limits on user activities specifically to fulfill job duties based on job descriptions.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO conducts a quarterly meeting with FOCUS IT Analysts to document monitoring activities.

EVIDENCE:
- Company calendar entries; RMS risk assessment; screenshots of ASA configuration; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS networks shall be segregated from production-level networks when migrating physical servers, applications or data to virtualized servers. *0894.01m2Organizational.7* This FOCUS policy is found in a section entitled '**Routing Controls'**. Evidence shall be the written policy; **firewall rules** screenshots and a supporting document entitled **'FOCUS Network Diagram'** to illustrate segregation. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that evidence and supporting documents are up-to-date and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold documented quarterly meetings with FOCUS IT Analysts to review and ensure that network configuration meets this policy; and
The FOCUS IT Analysts ensure that:
— The FOCUS Network Diagram is updated to illustrate compliance with this policy; and
— Networks are segregated from production-level networks when migrating physical servers, applications or data to virtualized servers, however FOCUS does not migrate any physical servers or applications to virtualized servers. FOCUS servers and applications are built from inception in a virtual session. FOCUS utilizes a closed, centralized environment (not a cloud environment).

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO conducts a quarterly meeting with FOCUS IT Analysts to document monitoring activities.

EVIDENCE:
- Company calendar entries; screenshots of ASA configuration; FOCUS network diagram; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 08 NETWORK PROTECTION

0805.01m1Organizational.12	HITRUST 01.m Segregation in Networks
0814.01n1Organizational.12	HITRUST 01.n Network Connection Control
0816.01w1System.1	HITRUST 01.w Sensitive System Isolation
0819.09m1Organizational.23	HITRUST 09.m Network Controls
0835.09n1Organizational.1	HITRUST 09.n Security of Network Services
0850.01o1Organizational.12	HITRUST 01.o Network Routing Control
0859.09m1Organizational.78	HITRUST 09.m Network Controls
0858.09m1Organizational.4	HITRUST 09.m Network Controls
0860.09m1Organizational.9	HITRUST 09.m Network Controls
0808.10b2System.3	HITRUST 10.b Input Data Validation
0806.01m2Organizational.12356	HITRUST 01.m Segregation in Networks
0894.01m2Organizational.7	HITRUST 01.m Segregation in Networks

09 Transmission Protection

POLICY:

FOCUS shall formally addresses multiple safeguards before allowing the use of information systems for information exchange. *0901.09s1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Information Exchange'**. Evidence shall be the written policy; The FOCUS CSO must approve all information exchange projects, as evidenced within documented **meeting minutes**. A screenshot of the **FOCUS Change Request Tracking System** shall be provided as evidence, and shall be utilized to track new or existing information exchange requests. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that information exchange requests meet all FOCUS policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information exchange to determine if, when using electronic communication applications or systems for information exchange, certain criteria are addressed.

PROCEDURES:

The FOCUS CSO ensures that:

— These policies are reviewed/modified/ratified no less than annually; and
— Before any network or system is utilized, encryption is confirmed prior to information exchanges; and
— Hold documented quarterly meetings with FOCUS IT Analysts to review and ensure that transmission safeguards are in place to fulfill this policy; and

The FOCUS IT Analysts ensures that:

— All security related software/procedural/protocols testing must be conducted on test environments; and
— SSL Certificates and applications that use them are compliant to deploy to the latest versions of SSL; and
— That prior/old implementations of SSL are disallowed from attempting to communicate with FOCUS systems or services; and
— SSL Certificates are current and active; and that renewal dates are entered into the company calendar.

MONITORING:

- The CSO monitosr the company calendar to ensure policy update compliance; and
- SSL certificate renewal calendar entries; and
- Test environment presentations by the FOCUS IT Analysts to the FOCUS CSO prior to 'golive' on production systems.

EVIDENCE:

- Company calendar entries; meeting minutes; test results of safeguards.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

POLICY:
Encryption of FOCUS data shall be used to protect covered information on mobile/removable media and across communication lines based on pre-determined criteria. *0903.10f1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Encryption'**. Evidence shall be the written policy; a screenshot of the FOCUS RMS **IT inventory system** will provide evidence of the tracking of any and all mobile/removable media to ensure encryption when containing covered information. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all covered information meets all FOCUS encryption policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the use of encryption to determine if the encryption policy addresses the use of encryption for protection of covered information transported by mobile or removable media, devices or across communication lines. Supporting encryption procedures address: (i) the required level of protection (e.g., the type and strength of the encryption algorithm required); and, (ii) specifications for the effective implementation throughout the organization (e.g., which solution is used for which business processes).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented meeting with the FOCUS IT Analysts is to take place quarterly; and
— Established requirements of encryption are documented and FOCUS IT Analysts are trained on these minimums:
    • 2,048 bit SSL/TLS v3.0 encryption for transport, with only the most modern handshake processes supported; and
    • Whole-disk encryption utilizing 128-bit AES encryption with a 256-bit key.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO monitors the documentation within FOCUS RMS Administration module/IT Inventory System to insure compliance.
- The CSO hosts quarterly review meetings.

EVIDENCE:
- Company calendar entries; meeting minutes; screenshot of FOCUS RMS Administration module/IT Inventory System illustrating current standards and research into the latest encryption methods.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that legal considerations, including requirements for electronic signatures, are addressed. *0925.09v1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. In the event FOCUS decides to change this policy, an update of all applicable FOCUS policies will be written to maintain compliance. Ongoing quality assurance monitoring mechanisms include documented **compliance research** by the FOCUS CSO shall be recorded on a monthly basis to ensure that all legal considerations regarding all identified Federal, State, accreditation and certification statutes and standards are met. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the current policy of FOCUS that e-signatures (i.e., 'Electronic Signatures') are not utilized.

PROCEDURES:
It is the current policy of FOCUS that e-signatures (i.e. 'Electronic Signatures') are not to be utilized; and
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Legal considerations are researched, by the CSO, on a monthly basis, within the FOCUS Administration module/Compliance system; and
— Should any Federal, State, or applicable Accrediting entities (such as URAC) or Certifying entities (such as HITRUST) require FOCUS to comply with statues, rules or standards, the FOCUS CSO is to incorporate these requirements into FOCUS policies & procedures in a timely manner to maintain compliance with said entity.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO monitors all Federal, State, accreditation and certifying entities monthly.

EVIDENCE:
- Company calendar; monthly compliance research documentation.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Approvals shall be obtained from the FOCUS CSO prior to using external public services, including instant messaging or file sharing. *0926.09v1Organizational.2* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is the policy of FOCUS that no external services are to be accessed by FOCUS employees utilizing FOCUS equipment for any FOCUS business except for instant messaging and file services provided to employees by FOCUS. At the time of this policy version, FOCUS provides all employees with **Microsoft Teams** for instant messaging and **Apple File Sharing** served from within the FOCUS data center for eligible employees. Evidence shall be the written policy prohibiting any FOCUS staff member from engaging in any electronic external public services with signature upon attesting to the FOCUS Security Policy and Procedure when initially hired and annually thereafter. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that attestations are on file for all FOCUS staff members. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees are provided training to read, attest and abide by the policy that no external services are to be accessed by FOCUS employees utilizing FOCUS equipment; and
— FOCUS provides approved secure services (such as instant messaging and file sharing) to be used solely for FOCUS business; and
— FOCUS provided file sharing services are reserved for Employees which have a business need (e.g., management team); and
— Any user that wishes to request any new or additional services may do so by sending a written email to: compliance@focushm.com.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO monitors, on a quarterly basis, all training attestations; and
- The CSO receives all incoming requests for any external public services for evaluation and proper assessment, testing and security review before considering the implementation of a company approved solution.

EVIDENCE:
- Company calendar; Email log of requests; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that stronger levels of authentication are implemented to control access from publicly accessible networks. *0927.09v1Organizational.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Two Factor Authentication' (TFA)**. Evidence shall be the written policy requiring TFA for FOCUS staff members and Peer Reviewers to access the FOCUS Review Management System. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all FOCUS staff members and Peer Reviewers are required to utilize TFA. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO, by assigning duties to the FOCUS IT Analysts ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Two factor authentication is implemented and maintained for all FOCUS Staff and contracted Peer Reviewers; and
— VPN Authentication and use are required for FOCUS Staff to access FOCUS systems.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO holds meetings on a quarterly basis with the FOCUS IT Analysts to review and confirm that stronger levels of authentication are in place.

EVIDENCE:
- Company calendar; meeting minutes; screenshots of two factor authentication and VPN authentication.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that stronger controls are implemented to protect certain electronic messages, and electronic messages are protected throughout the duration of its end-to-end transport path using cryptographic mechanisms unless protected by alternative measures. *0928.09v1Organizational.45* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring encryption with the transport of any protected information; a requirement for the FOCUS CSO to document approval of all new information transportation mediums, and a **screenshot** showing the SSL certificate information for all electronic transport mediums currently in use. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that SSL certificates are current, awareness of SSL certificate expiration and assurance that all protected information is encrypted during transport. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the use of electronic messaging and determine stronger controls, such as electronic signatures, are implemented to protect certain electronic messages (e.g., those containing PII or other covered information). Electronic messages are protected throughout the duration of its end-to-end transport path using cryptographic mechanisms to protect message integrity and confidentiality unless protected by alternative measures (e.g., physical controls).

PROCEDURES:
The FOCUS CSO, by assigning duties to the FOCUS IT Analysts ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Electronic mail systems used by FOCUS provide end-to-end encryption, including secure webmail; and
— The FOCUS CSO holds quarterly meetings with the FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
- The CSO monitors the company calendar to ensure policy update compliance; and
- The CSO holds quarterly meetings to confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes; screenshots of email encryption settings and webmail authentication mechanisms.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall never send unencrypted sensitive information by end-user messaging technologies (e.g., email, instant messaging, and chat). *0929.09v1Organizational.6* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy prohibiting any FOCUS staff member from transferring or attempting to transfer sensitive information by any means other than what mechanisms are provided, with attestations of understanding to the FOCUS Security Policy and Procedure when initially hired and annually thereafter. Further evidence shall be maintained based on **screenshots** of end-user systems illustrating that no web browser or email tools are available to the end-user. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that attestations are on file for all FOCUS staff members. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training for all FOCUS Staff and contracted Peer Reviewers to confirm that they have read/understand/attest/comply with this policy; and
— Provide supplemental training, should a FOCUS Staff Member or Peer Reviewer fail in complying with this policy; and
— The FOCUS IT Analyst Team ensures that company systems and secure environments shall only have approved software for processing sensitive information.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Ensures that all training attestations are reviewed quarterly; and
- Conducts documented meetings with FOCUS IT Analysts to confirm security of configured end-user systems.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall take specific steps to ensure the confidentiality and integrity of electronic commerce are maintained. *0938.09x1Organizational.1*
These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that attestations for the FOCUS Security Policy and Procedure are on file for all FOCUS staff members. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that electronic commerce in any form is prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— All FOCUS Staff Members and contracted Peer Reviewers are to receive training, read/understand/attest/comply with this policy; and
— In the event this policy were to be modified to allow electronic commerce, the appropriate specific steps to ensure the confidentiality and integrity of electronic commerce would be added.

MONITORING:
The FOCUS CSO:
• Monitors the company calendar to ensure policy update compliance.

EVIDENCE:
• Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that data involved in electronic commerce and online transactions is checked to determine if it contains covered information. *0943.09y1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all data types are categorized and determined to have (or not have) covered information. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that electronic commerce in any form is prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— All FOCUS Staff Members and contracted Peer Reviewers are to receive training, read/understand/attest/comply with this policy; and
— In the event this policy were to be modified to allow electronic commerce, the appropriate specific steps to ensure the confidentiality and integrity of electronic commerce would be added.

MONITORING:
The FOCUS CSO:
• Monitors the company calendar to ensure policy update compliance.

EVIDENCE:
• Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that security is maintained through all aspects of the transaction. *0944.09y1Organizational.2* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy, whereby all covered information transactions must be acquired (receiving transmission), processed, stored and transmitted securely. Evidence shall be recorded that includes reports generated by the **FOCUS Change Request Tracking System** which will address end-to-end technological security aspects as well as stakeholder responsibilities to ensure secure transactions; FOCUS staff member and Peer Reviewer signature upon attesting to the FOCUS Security Policy and Procedure when initially hired and annually thereafter. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all transactions with covered information are assessed to ensure secure processing. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to online transactions to determine if security is maintained through all aspects of the transaction, ensuring that: (i) user credentials of all parties are valid and verified; (ii) the transaction remains confidential; and, (iii) privacy associated with all parties involved is retained.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— All FOCUS Staff Members and contracted Peer Reviewers are to receive training, read/understand/attest/comply with this policy and a commitment to not circumvent or undermine the security of any transactions; and
— Documented meetings with the FOCUS IT Analysts are held quarterly to confirm that:
- Access to FOCUS systems and network are secure; and
- SSL/TLS certificates are renewed, valid and active; and
- Web browser users show valid security certificates upon use to ensure encryption during transport.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conducts meetings with FOCUS IT Analysts quarterly to monitor and assure that security is maintained through all aspects of all transactions.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL). *0945.09y1Organizational.3* This FOCUS policy is found in a section entitled '**Encryption'**. Evidence shall be the written policy, whereby all covered information transactions must be electronically secured by Secure Socket Layer (SSL) Certificates and **screenshots** and specifications of **FOCUS secure certificates** are on file. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that secure protocols are maintained through all aspects of the transaction. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are to receive training, read/understand/attest/comply with this policy; and
— Documented meetings with the FOCUS IT Analysts are held quarterly to confirm that:
- Access to FOCUS systems and network are secure; and
- SSL/TLS certificates are renewed, valid and active; and
- Web browser users show valid security certificates upon use to ensure encryption during transport.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conduct smeetings with FOCUS IT Analysts quarterly to monitor and assure that protocols used to communicate between all involved parties are secured using cryptographic techniques (e.g., SSL)

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall not send PII/PHI over facsimile (FAX), unless it cannot be sent over other, more secure, channels (e.g., delivery by hand, secure email). *0961.09v1Organizational.7* Evidence shall be the written policy, whereby facsimile is not to be used for any PII/PHI data; and that all covered information transactions must be electronically secured by Secure Socket Layer (SSL) Certificates for electronic transfer; and FOCUS staff member and Peer Reviewer signature upon training and attesting to the FOCUS Security Policy and Procedure when initially hired and annually thereafter. Further evidence shall be screenshots of SSL certificates on file. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that secure protocols are maintained through all aspects of the transaction. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that at no time shall PHI/PII be printed on paper nor transmitted via facsimile machine.

PROCEDURES:
It is FOCUS policy that at no time will PHI/PII be printed on paper nor transmitted via facsimile machine.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Staff Members and contracted Peer Reviewers are to receive training, read/understand/attest/comply with this policy; and
— Documented meetings with the FOCUS IT Analysts are held quarterly to confirm that:
- Facsimile systems (via email, over-internet or hardware) are prohibited; and
- SSL/TLS certificates are verified and active for transmission of PHI/PII.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conducts meetings with FOCUS IT Analysts quarterly to monitor and assure that protocols used to communicate PHI/PII are secured using cryptographic techniques (e.g., SSL)

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall establish terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to (i) access the information system from external information systems; and (ii) process, store or transmit organization-controlled information using external information systems. *0911.09s1Organizational.2* This FOCUS policy is detailed in a separate policy entitled '**Terms of Use v2.0.pdf'**. Evidence shall be the written policy, whereby FOCUS shall author 'terms and conditions' to be approved by the CEO and CSO and available within the FOCUS Review Management System and the FOCUS public website available for any stakeholder to read 24/7/365. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** by the FOCUS CEO and FOCUS CSO recorded on a quarterly basis to ensure that FOCUS Terms and Conditions language continues to meet Federal and State statutes as well as client-company contractural requirements. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information exchange to determine if the organization establishes terms and conditions, consistent with any trust relationship established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to (i) access the information system from external information systems; and (ii) process, store or transmit organization-controlled information using external information systems.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS Policy entitled 'Terms of Use v2.0.pdf' is to be easily available for viewing 24/7/365 within the FOCUS RMS and the FOCUS public website; and
— FOCUS establishes terms and conditions within client-company contracts when clients desire to interoperate with the FOCUS Review Management System (RMS) so that clients may submit protected data to FOCUS and FOCUS may submit protected data to the client, allowing connectivity through an automated Application Processing Interface (API); and
— FOCUS provides training to all users of the FOCUS system (both Staff Members and contract Peer Reviewers) to read/understand/attest/comply with the FOCUS terms and conditions policy.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that all users have attested to policies; and
- Monitors client-company contracts to ensure that language regarding terms of use when interoperating via an API is engaged.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief security Officer

POLICY:
FOCUS shall ensure that cryptography is used to protect the confidentiality and integrity of remote access sessions to the internal network and to external systems. *0912.09s1Organizational.4* FOCUS requires virtual private network (VPN) access to the FOCUS network by FOCUS staff members via required **Security Appliances** (hardware firewalls) to ensure encrypted transport of information between remote systems and end users; and **screenshots** of the configuration of FOCUS security appliances shall be on file. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** by the FOCUS CEO and FOCUS CSO recorded on a quarterly basis to ensure that FOCUS firewalls are properly configured. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are to be held with FOCUS IT Analysts to review and confirm encryption; and
The FOCUS IT Analysts ensures that:
— The FOCUS Security Appliance (ASA) is to be configured to require VPN connectivity with encryption and access privileges so that remote access sessions are delivered to end user systems encrypted; and
— Screenshots of configuration and screenshots of VPN access are stored in the RMS as evidence.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conducts documented quarterly meetings with FOCUS IT Analysts to review and confirm encryption.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that strong cryptography protocols are used to safeguard covered information during transmission over less trusted / open public networks. *0913.09s1Organizational.5* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring **strong encryption** (2,048 bit or higher) with certificates acquired from nationally recognized certificate signing authorities; a **screenshot** showing the SSL certificate information for all electronic transport mediums employed by FOCUS. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that SSL certificates are current, awareness of SSL certificate expiration and assurance that all protected information is encrypted during transport. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information exchange to determine if formal procedures are defined to encrypt data in transit including use of strong cryptography protocols to safeguard covered information during transmission over less trusted/open public networks.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are to be held with FOCUS IT Analysts to review and confirm encryption strength; and
The FOCUS IT Analysts ensures that:
— The FOCUS Security Appliance (ASA) is to be configured to require VPN connectivity with strong encryption protocols (2,048 bit or higher) so that remote access sessions are delivered to end user systems strongly encrypted; and
— Certificates acquired from nationally recognized certificate signing authorities; and
— Screenshots of configuration and screenshots of VPN access are stored in the RMS as evidence.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conducts documented quarterly meetings with FOCUS IT Analysts to review and confirm strong, validated encryption.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that communication protection requirements, including the security of exchanges of information, is the subject of policy development and compliance audits. 0914.09s1Organizational.6 These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring the topic of security to be included with all policy development, as well as inclusion in FOCUS' required monthly compliance research process; and a **screenshot** showing the FOCUS compliance audit screen. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that security is a top consideration regarding all communications and exchanges of information within all systems and with all stakeholders. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information exchange to determine if the organization ensures that communications protection requirements, including the security of exchanges of information, is the subject of policy development (see also 04.a and 04.b) and compliance audits (see 06.g) consistent with relevant legislation.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are to be held with FOCUS IT Analysts to review and confirm communication protection requirements, including encryption, authentication and automated system transmissions in an effort to acquire suggestions and input on best practices as well as gaps to incorporate into future versions of training materials and policy/procedure development; and
— Every available security topic is researched/discussed/evaluated and incorporated into future FOCUS training guides and Policies & Procedures.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Conducts documented quarterly meetings with FOCUS IT Analysts for future training & policy updates; and
- Conducts research to ensure that the latest best practices and methods to ensure communication protection is incorporated into future training & policy updates.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 09 TRANSMISSION PROTECTION

0901.09s1Organizational.1	HITRUST 09.s Information Exchange Policies and Procedures
0903.10f1Organizational.1	HITRUST 10.f Policy on the Use of Cryptographic Controls
0925.09v1Organizational.1	HITRUST 09.v Electronic Messaging
0926.09v1Organizational.2	HITRUST 09.v Electronic Messaging
0927.09v1Organizational.3	HITRUST 09.v Electronic Messaging
0928.09v1Organizational.45	HITRUST 09.v Electronic Messaging
0929.09v1Organizational.6	HITRUST 09.v Electronic Messaging
0938.09x1Organizational.1	HITRUST 09.x Electronic Commerce Services
0943.09y1Organizational.1	HITRUST 09.y Online Transactions
0944.09y1Organizational.2	HITRUST 09.y Online Transactions
0945.09y1Organizational.3	HITRUST 09.y Online Transactions
0961.09v1Organizational.7	HITRUST 09.v Electronic Messaging
0911.09s1Organizational.2	HITRUST 09.s Information Exchange Policies and Procedures
0912.09s1Organizational.4	HITRUST 09.s Information Exchange Policies and Procedures
0913.09s1Organizational.5	HITRUST 09.s Information Exchange Policies and Procedures
0914.09s1Organizational.6	HITRUST 09.s Information Exchange Policies and Procedures

10 Password Management

ACCOUNT SECURITY POLICY:

All accounts on FH resources will be authorized by the FH Chief Security Officer before activation. Accounts are for use by only the authorized individual and are not to be shared. Passwords and private keys should never be shared with anyone (this includes supervisors, coworkers, and spouses).
Users must maintain the secrecy of private passwords associated with their account. Users must regularly change their secure passwords (monthly is FH policy). If you suspect the secrecy of a password associated with any FOCUS service may have been compromised, contact the FH Security Officer or FH IT Technical Support team immediately.
Should users forget their password, users are directed to call the FH IT Technical Support team immediately.
New users must set a new password during the initial login. Accounts are centrally managed and monitored periodically and a review is required annually.
FH does not allow clear-text passwords (static passwords over an unencrypted channel) for remote access to any systems.
All attempts (both successful and unsuccessful) to login to the FH Review Management System are recorded. Upon discontinuance of employment with FH, your account will no longer function; do not attempt to login.

FOCUS policy requires that all USER IDs must be a minimum of 8 characters in length. Upper and lower case alpha characters are allowed. Each user shall be issues a unique USER ID (Account Name).

FOCUS policy requires that all passwords expire every thirty (30) days. Passwords shall be a minimum of 8 characters in length and have at least one numeric character. Upper and lower case alpha characters are allowed and at least one upper case character is required. Use of any previous 10 passwords are not permitted. When Users attempt to update (renew/change) their password, the 'new' password is automatically checked against a known list of passwords which have been involved in data breaches, and shall not be permitted.

Should a user attempt 5 times to login into the system, the user is notified that they are no longer able to login without calling a toll-free number (866-561-9542) to speak with a FOCUS IT Analyst to confirm their identity and re-activate their login privileges. Should this occur, a new password must be established.

It is FOCUS policy that users shall be provided initial (new) or modified user account names and passwords via a secure email solution. FOCUS shall send account name/password encrypted email to Users with automated 'read-receipts' activated for monitoring and documentation purposes.

PROCEDURES:

The FOCUS CSO ensures that:
— All accounts on FH resources will be authorized by the FH Chief Security Officer before activation.
— Users must change their password every thirty (30) days.
— If a User suspects the secrecy of a password associated with any FOCUS service may have been compromised, contact the FH Security Officer or FH IT Technical Support team immediately.
— Should a User forget their password, users are directed to call the FH IT Technical Support team immediately.
— FOCUS is to ensure, through rules on-screen in software, that all USER IDs must be a minimum of 8 characters in length. Upper and lower case alpha characters are allowed. Each user is to be issues a unique USER ID (Account Name).
— Passwords are to be a minimum of 8 characters in length and have at least one numeric character. Upper and lower case alpha characters are allowed and at least one upper case character is required. Use of any previous 10 passwords are not permitted.
— When Users attempt to update (renew/change) their password, the 'new' password is automatically checked against a known list of passwords which have been involved in data breaches, and prevent the User to utilize the attempted password.
— Should a user attempt 5 times to login into the system, the user is notified that they are no longer able to login without calling a toll-free number (866-561-9542) to speak with a FOCUS IT Analyst to confirm their identity and re-activate their login privileges. Should this occur, a new password must be established.
— Users are to be securely emailed their account information (initial and any modified account name/password) using an encrypted email solution.
— FOCUS is to send account name/password encrypted email to Users with automated 'read-receipts' activated for monitoring and documentation purposes.
— Passwords are not to be displayed on screens or reports.

POLICY:
FOCUS shall ensure that passwords are not displayed when entered. *1002.01d1System.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring passwords to not be displayed; and a **screenshot** showing the Virtual Private Network (VPN) and FOCUS Review Management System (RMS) password entry fields do not display legible characters. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are to be held with FOCUS IT Analysts to inspect login prompts to ensure that passwords; and
— Confirm that passwords are not displayed within the RMS system after being established by end users.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors meeting minutes to ensure that any suspected instances of password visibility have been modified to prevent visibility.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that user identities are verified prior to performing password resets. *1003.01d1System.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring passwords to not be provided to end-users without verification requirements per stakeholder type; and a **screenshot** showing the rules within the FOCUS Review Management System **password reset function** for FOCUS IT Analysts to document each password reset request. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training for FOCUS IT Analysts, whom take technical support calls when end-users request password resets, must read/understand/attest and comply with this policy:
- If the end user is a client-company associate, the FOCUS IT Analyst must first receive an email from the direct report of the client company staff member, with the direct report request to have the client-company staff member's password reset; and
- If the end user is a FOCUS Staff Member, the FOCUS IT Analyst must receive an email from the direct report of the staff member; and
- If the end user is a FOCUS contracted Peer Reviewer, the FOCUS IT Analyst must receive an email from the Chief Medical Officer of FOCUS.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall maintain a list of commonly used, expected or compromised passwords, and updates the list at least every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly; verifies, when users create or update passwords, that the passwords are not found on FOCUS-defined list of commonly used, expected or compromised passwords; allows users to select long passwords and pass-phrases, including spaces and all printable characters; and employs automated tools to assist the user in selecting strong passwords and authenticators. *1004.01d1System.8913* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring passwords to meet all criteria for this standard; and a **screenshot** showing the rules within the FOCUS Review Management System **password creation/modification function** which all stakeholders must utilize when initially establishing or changing their password. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password management and determine whether the organization: (i) maintains a list of commonly used, expected or compromised passwords, and updates the list at least every 180 days and when organizational passwords are suspected to have been compromised, either directly or indirectly; (ii) verifies, when users create or update passwords, that the passwords are not found on the organization-defined list of commonly-used, expected or compromised passwords; (iii) allows users to select long passwords and passphrases, including spaces and all printable characters; and, (iv) employs automated tools to assist the user in selecting strong passwords and authenticators.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training for FOCUS IT Analysts, to ensure that they have read/understand/attested and comply with this policy; and
The FOCUS IT Analysts ensures that:
— Within the RMS in the Administration module/IT Inventory System, a list of commonly used, expected or compromised passwords is maintained; and
— The FOCUS IT Analysts are to update the list at least every 180 days; and
— When organizational passwords are suspected to have been compromised, either directly or indirectly; verifies, when users create or update passwords, that the passwords are not found on FOCUS-defined list of commonly used, expected or compromised passwords; and
— Allows users to select long passwords and pass phrases, including spaces and all printable characters; and
— Employs automated tools to assist the user in selecting strong passwords and authenticators, including a graphical rating system of the users' new password prior to accepting the new password.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy; and
- Monitors the inventory of common passwords that the FOCUS IT/Analysts have generated for quality and completeness.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; organizational inappropriate password inventory report.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall transmit passwords only when cryptographically protected and stores passwords using an approved hash algorithm. *1005.01d1System.1011* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Encryption'**. Evidence shall be the written policy requiring that passwords are cryptographically protected by a nationally recognized secure socket layer (SSL) certificate and that password storage within the FOCUS Review Management System uses AES-256 algorithm encryption when stored; and a **screenshot** showing the SSL certificate specifications. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented meeting with the FOCUS IT Analysts to review and ensure compliance; and
— Ensures that passwords are transmitted only when cryptographically protected, such as when a client-company end user enters their unreadable password entry field (i.e. '••••••') in a web browser, that it is always transmitted to FOCUS servers encrypted during transport (e.g., via strong SSL encryption); and
— Ensures that passwords are stored in a one-way hash (meaning the password can be encrypted but never decrypted), which means that passwords may be reset but may never be recovered.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews meeting minutes and ensure that this policy is enforced for all stakeholders.

EVIDENCE:
- Company calendar; meeting minutes; screenshots of SSL certificate evidence from end-user web browsers.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that password policies, applicable to mobile devices, are documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and prohibit the changing of password/PIN lengths and authentication requirements. *1022.01d1System.15* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that users not modify password/PIN lengths and authentication requirements; and that training and attestation to the FOCUS Security Policy and Procedure be on file for every FOCUS staff member and Peer Reviewer upon initial hire and annually thereafter. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all FOCUS staff members and Peer Reviewers have attested to the FOCUS security policy and procedure. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password requirements on mobile devices to determine if password policies, applicable to mobile devices, are documented and enforced through technical controls on all company devices or devices approved for BYOD usage, and prohibit the changing of password/PIN lengths and authentication requirements for reading e-mail, composing documents, or surfing the Internet.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented quarterly meeting with the FOCUS IT Analysts to review and verify compliance with this policy; and
— Training is to be provided to all FOCUS Staff Members and contracted Peer Reviewers that they read/understand/attest and comply with this policy; and
The FOCUS IT Analysts ensure that:
— Remote management of mobile devices are to disallow end-users from modifying password lengths, PIN lengths and authentication requirements.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews quarterly meeting minutes from FOCUS IT Analyst discussions and if necessary, provide additional training to ensure this policy is enforced.

EVIDENCE:
- Company calendar; meeting minutes; screenshots of Password/PIN requirements for mobile users.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall avoid the use of third parties or unprotected (clear text) electronic mail messages for the dissemination of passwords. *1014.01d1System.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that FOCUS IT Staff are never to use unprotected email to disseminate initial or subsequent passwords to end-users; and that training and attestation to the FOCUS Security Policy and Procedure be on file for every FOCUS IT staff member and Peer Reviewer upon initial hire and annually thereafter; and a screenshot of the account creation screen in the FOCUS Review Management System reiterating the proper steps of securely disseminating passwords to end-users. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all FOCUS staff members and Peer Reviewers have attested to the FOCUS security policy and procedure. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented quarterly meeting with the FOCUS IT Analysts to review and verify compliance with this policy; and
— Training is to be provided to FOCUS IT Analysts that they read/understand/attest and comply with this policy; and
The FOCUS IT Analysts ensure that:
— Electronic mail communications are to always be encrypted in sending initial passwords to end users; and
— Send test secure emails to the CSO quarterly to confirm compliance.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews quarterly meeting minutes from FOCUS IT Analyst discussions, and if necessary, provide additional training ensure this policy is enforced.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; secure email tests.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS ensures that users acknowledge receipt of passwords. *1015.01d1System.14* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that FOCUS IT Staff confirms that the intended recipient of a password acknowledges receipt before the user account is active; and that training and attestation to the FOCUS Security Policy and Procedure be on file for every FOCUS IT staff member and Peer Reviewer upon initial hire and annually thereafter; and a screenshot of the account creation screen in the FOCUS Review Management System reiterating the proper steps of acquiring acknowledgement from end users and activating the account; and that this is an element of the FOCUS staff member **onboarding** policy and procedure. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all FOCUS staff members and Peer Reviewers have attested to the FOCUS security policy and procedure. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented quarterly meeting with the FOCUS IT Analysts to review and verify compliance with this policy; and
— Training is to be provided to FOCUS IT Analysts that they read/understand/attest and comply with this policy; and
The FOCUS IT Analysts ensures that:
— Electronic mail communications are to always be sent with a 'read receipt' function to confirm that the end user acknowledged receipt of the initial password; and
— Send test secure emails to the CSO quarterly with 'read receipt' activated to confirm compliance.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Review squarterly meeting minutes from FOCUS IT Analyst discussions, and if necessary, provide additional training ensure this policy is enforced.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; secure email tests with documented 'read receipts'.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall change passwords for default system accounts, at first logon following the issuance of a secure temporary password, when there is a suspected compromise, and no less than every ninety (90) days for regular accounts or 60 days for privileged (i.e., administrator accounts). *1031.01d1System.34510* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Passwords'**. Evidence shall be the written policy requiring that the FOCUS Review Management System prompts users 30 days prior to access discontinuance with a notice that a password change is required; and a **screenshot** of the on-screen notification to end-users to this effect; and a **screenshot** of the new user account creation function illustrating the 60 or 90 day differentiation per privilege set. Ongoing quality assurance monitoring mechanisms include review of automated **reports** generated by the FOCUS Review Management System so that password reset frequencies can be audited by the FOCUS CSO, recorded in **meeting minutes** on a quarterly basis to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password management and determine if the organization has implemented the following controls to allocate and maintain the security of password: (i) passwords are changed whenever there is any indication of possible system or password compromise; (ii) default vendor passwords are altered following installation of systems or software; (iii) temporary passwords are changed at the first log-on; and, (iv) require immediate selection of a new password upon account recovery.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented quarterly meeting with the FOCUS IT Analysts to review and verify compliance with this policy; and
FOCUS IT Analysts ensures that:
— When adding a new end-user, the RMS requires the end user to change the default password, with the required password complexity (defined elsewhere within this document), the first time the user logs in before accessing any data; and
— In the event of a suspected compromise, the end-user account must be adjusted to require a password upon their next login attempts; and
— End user accounts that are not administrators must require being reset every 90 days; and
— End user accounts that are administrators must require being reset ever 60 days.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews quarterly meeting minutes from FOCUS IT Analyst discussions, and if necessary, provide additional training ensure this policy is enforced.

EVIDENCE:
- Company calendar; meeting minutes; screenshot of forced end-user password update routine.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that identification codes used in conjunction with passwords for electronic signatures are protected. *1010.01d2System.5*
These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is the policy of FOCUS health that electronic signatures are prohibited. Evidence shall be the written policy requiring that passwords are cryptographically protected by a nationally recognized secure socket layer (SSL) certificate and that password storage within the FOCUS Review Management System uses AES-256 algorithm encryption when stored; and a **screenshot** showing the SSL certificate specifications. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password management and determine if persons who use electronic signatures, based upon use of identification codes in combination with passwords, employ controls to ensure security and integrity.

PROCEDURES:
It is the policy of FOCUS health that electronic signatures are prohibited.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Should electronic signatures be allowed, this policy will be updated to ensure that Identification codes used in conjunction with passwords for electronic signatures are protected.

MONITORING:
The FOCUS CSO:
• Monitors the company calendar to ensure policy update compliance.

EVIDENCE:
• Company calendar; effective policy.

RESPONSIBLE PARTY:
• FOCUS IT Analyst

POLICY:
FOCUS shall ensure that passwords are not included in automated log-on processes. *1006.01d2System.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that the FOCUS Review Management System disallows automated password retention features; and a **screenshot** of the on-screen login prompt showing no such feature available to end users; and that this be an item including in the FOCUS **onboarding** policy and procedure. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this policy is enforced. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensure that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training for the FOCUS IT Analysts is provided to ensure compliance with this policy; and
— Hold a documented meeting quarterly with FOCUS IT Analysts to ensure compliance; and
The FOCUS IT Analysts ensures that:
— All FOCUS Employee systems must not allow the operating-system based option to store login account information nor password information for automated logons.

MONITORING:
- The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training attestations to ensure compliance.

EVIDENCE:
- Company calendar; effective policy; training attestations; screenshot of login with disabled (or missing) option for automated login.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that passwords are encrypted during transmission and storage on all system components. *1007.01d2System.2* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that passwords are cryptographically protected by a nationally recognized secure socket layer (SSL) certificate and that password storage within the FOCUS Review Management System uses AES-256 algorithm encryption when stored; and that VPN passwords entry is also cryptographically protected when credentialing into the FOCUS security appliance (firewall); and **screenshots** showing the SSL certificate specifications (RMS) and the cryptography of the FOCUS security appliance (VPN). Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** between the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that the encryption secure certificates are active and current. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented meeting quarterly with the FOCUS IT Analysts to review and ensure compliance; and
— Ensures that passwords are transmitted only when cryptographically protected, such as when a client-company end user enters their unreadable password entry field (i.e. '••••••') in a web browser, that it is always transmitted to FOCUS servers encrypted during transport (e.g., via strong SSL encryption); and
— Ensures that passwords are stored in a one-way hash (meaning the password can be encrypted but never decrypted), which means that passwords may be reset but may never be recovered.

MONITORING:
The FOCUS CSO:
• Monitors the company calendar to ensure policy update compliance; and
• Reviews meeting minutes and ensure that this policy is enforced for all stakeholders.

EVIDENCE:
• Company calendar; meeting minutes; screenshots of SSL certificate evidence from end-user web browsers.

RESPONSIBLE PARTY:
• FOCUS IT Analyst

POLICY:
FOCUS shall ensure that users sign a statement acknowledging their responsibility to keep passwords confidential. *1008.01d2System.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Passwords'**. Evidence shall be the written policy requiring that passwords are to be kept confidential, and to never divulge passwords to anyone; and attestations to reading and understanding the **FOCUS Confidentiality Agreement(s)** that end-users must initially and annually sign. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that all users have signed the FOCUS confidentiality agreement. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password management and determine if users sign a statement to keep personal passwords confidential and to keep group passwords solely within the members of the group.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— End-users are provided initial and annual training to never divulge passwords to anyone by reading/understanding/attesting to training and attesting to a separate document which reiterates this requirement and records their attestation date/time/signature image.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews training logs and attestations to ensure that this policy is enforced for all end users.

EVIDENCE:
- Company calendar; meeting minutes; attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that temporary passwords are unique and not guessable. *1009.01d2System.4* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that temporary passwords are to meet specified nomenclature requirements, are unique, and not 'guessable'; and a **screenshot** will be on file illustrating a sample password. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that temporary passwords meet FOCUS policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hold a documented meeting quarterly with the FOCUS IT Analysts to review and ensure compliance; and
— Ensures that temporary passwords are generated by the RMS, highly randomly, with a minimum of 10 characters which include alpha characters (a-z) at least two numbers (0-9), at least one special character (!@#$%^&*) and at least one capital alpha character (A, Z).

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Reviews meeting minutes with FOCUS IT Analysts to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; effective policy.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that electronic signatures that are not based upon biometrics employ at least two distinct identification components that are administered and executed. *1027.01d2System6* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is the policy of FOCUS that electronic signatures are prohibited. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to password management to determine whether electronic signatures that are not based upon biometrics: (i) employ at least two distinct identification components (e.g., user ID and password)–when an individual executes a series of signings during a single continuous period of controlled system access, the first signing is executed using all electronic signature components, and subsequent signings are executed using at least one electronic signature component (when an individual executes one or more signings not performed during a single, continuous period of controlled system access, each signing is executed using all of the electronic signature components); and, (ii) be administered and executed to ensure that attempted use of an individuals electronic signature by anyone other than its genuine owner requires collaboration of two or more individuals (e.g., system administrator and supervisor).

PROCEDURES:
It is the policy of FOCUS that electronic signatures are prohibited.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— In the event FOCUS intends to support the use of electronic signatures, this policy will be updated to ensure that electronic signatures that are not based upon biometrics employ at least two distinct identification components that are administered and executed.

MONITORING:
The FOCUS CSO:
• Monitors the company calendar to ensure policy update compliance.

EVIDENCE:
• Company calendar; effective policy.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 10 PASSWORD MANAGEMENT

1002.01d1System.1	HITRUST 01.d User Password Management
1003.01d1System.3	HITRUST 01.d User Password Management
1004.01d1System.8913	HITRUST 01.d User Password Management
1005.01d1System.1011	HITRUST 01.d User Password Management
1022.01d1System.15	HITRUST 01.d User Password Management
1014.01d1System.12	HITRUST 01.d User Password Management
1015.01d1System.14	HITRUST 01.d User Password Management
1031.01d1System.34510	HITRUST 01.d User Password Management
1010.01d2System.5	HITRUST 01.d User Password Management
1006.01d2System.1	HITRUST 01.d User Password Management
1007.01d2System.2	HITRUST 01.d User Password Management
1008.01d2System.3	HITRUST 01.d User Password Management
1009.01d2System.4	HITRUST 01.d User Password Management
1027.01d2System.6	HITRUST 01.d User Password Management

11 Access Control

Audit and Accountability Policy

In an effort to meet HIPAA guidelines and provide accountability to stakeholders, FH has implemented the following features into the Review Management System:

- Automated recording of all users' logins to the system, including date, time & user name; and
- Automated recording of record creation date, time and user name; and
- Automated recording of record editing date, time and user name; and
- Automated recording of all field (data point) changes by date, time and user name.

Further, all data recorded by the RMS is able to be reported by staff with appropriate security clearances.

User Access Policy

All new users of the FH Review Management System requires a login account name and password. Each new FH staff member or peer reviewer is assigned a login account name and password only after signing the FH non-disclosure Agreement, having been 'cleared' on a background check and cleared of the OIG and GSA exceptions list websites, and receiving training on FH security policies & procedures. When a new employee is hired at a FH client-company, creation of an account name and password may only be granted upon receipt of an email from the new employees' manager indicating the client-company staff members' name, email address and phone number.

FOCUS Background Check Policy

Prospective employees desiring to work for FOCUS are required to agree to allow FOCUS to complete background checks before the employment process is completed. These background checks may include criminal, financial or other information gathered in an effort to determine eligibility for employment with FOCUS. Additionally, each staff member must 'clear' the OIG & GSA Exceptions search on their respective websites. Any staff member found on the OIG or GSA Exclusions lists will be removed. The decision for eligibility or ineligibility is determined by the hiring manager, and in the event of an adverse decision, the prospective employee may request that the Chief Executive Officer review their application and the results of the background checks. FOCUS reserves the right, after the completion of the employment process, to conduct additional background checks during tenure with FOCUS on an annual basis. FOCUS will always abide by legal requirements regarding disclosure of intent to acquire background checks, as well as any approvals that may be required on your part. OIG and GSA checks shall be executed and recorded every month for each Staff Member and contracted Peer Reviewer until their departure from FOCUS.

Removal of Access

Upon notification by FOCUS Senior Staff, the Chief Security Officer shall direct FOCUS IT staff to remove access privileges from all FOCUS systems. Confirmation of removal will be conducted by the Chief Security Officer. Removal once order by Chief Security Officer must take place within 15 minutes or less.

POLICY:
FOCUS shall ensure that user identities are verified prior to establishing accounts. *1106.01b1System.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that user identity must be verified before creation of accounts to access FOCUS systems; and a **screenshot** will be on file illustrating the account setup function and evidence retained of identity verification. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that end-user identity verification meet FOCUS policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user registration and determine if proper identification is required for requests to establish information system accounts and approval of all such requests.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training for FOCUS IT Analysts, whom take requests to add end-users, must read/understand/attest and comply with this policy:
- If the end user is a client-company associate, the FOCUS IT Analyst must first receive an email from the direct report of the client company staff member, with the direct report request to have the client-company staff member added to the RMS and
- If the end user is a FOCUS Staff Member, the FOCUS IT Analyst must receive an email from the direct report of the staff member; and
- If the end user is a FOCUS contracted Peer Reviewer, the FOCUS IT Analyst must receive an email from the Chief Medical Officer of FOCUS.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance at least annually; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that default and unnecessary system accounts are removed, disabled, or otherwise secured (e.g., the passwords are changed and privileges are reduced to the lowest levels of access). *1107.01b1System.2* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring the CSO to review all accounts and ensure the absence of default and unnecessary system accounts are removed, disabled or otherwise secured; and a **screenshot** will be on file illustrating the account setup function and privilege options for user accounts. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that the default or unnecessary system account inventory meet FOCUS policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly documented meetings with the FOCUS IT Analysts are scheduled; and
— Training for FOCUS IT Analysts must read/understand/attest and comply with this policy:
- Upon acquisition of new hardware or software which requires account access, the default systems accounts are removed or disabled and replaced with a documented user account and password and privileges reduced to the lowest levels of access.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that account managers are notified when users' access rights change (e.g., termination, change in position) and modify the user's account accordingly. *1108.01b1System.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring that upon notification of a FOCUS staff member or Peer Reviewer being dismissed or a modification in their position, assessment by FOCUS IT Analysts to assure that the end-user privileges are adjusted as necessary; and a **screenshot** will be on file illustrating the account setup function and privilege options for user accounts. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that current end-user account privileges meet FOCUS policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user account administration and determine if account managers are notified when users are terminated or transferred, their information system usage or need-to-know/need-to-share changes, or when accounts (including shared/group, emergency, and temporary accounts) are no longer required.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly documented meetings with the FOCUS IT Analysts are scheduled; and
— Changes to access rights are maintained in an inventory for future review and reporting purposes; and
— Training for FOCUS IT Analysts must read/understand/attest and comply with this policy:
- Upon receiving a request to modify user access rights, the respective individual's direct report must provide an email, with identifying information, with instructions (such as termination, change in position or change in privileges) before proceeding.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that user registration and de-registration, at a minimum, communicate relevant policies to users and require acknowledgement (e.g. signed or captured electronically), check authorization and minimum level of access necessary prior to granting access, ensure access is appropriate to the business and/or clinical needs (consistent with sensitivity/risk and does not violate segregation of duties requirements), address termination and transfer, ensure default accounts are removed and/or renamed, remove or block critical access rights of users who have changed roles or jobs, and automatically remove or disable inactive accounts. *1109.01b1System.479* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be the written policy requiring compliance with the elements of this standard; and that **evidence is collected** and stored in the FOCUS RMS to justify the necessary end-user privilege set; and a **screenshot** will be on file illustrating the account setup function and privilege options for user accounts. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A documented meeting is to be held quarterly with FOCUS IT Analysts to ensure compliance; and
— Training of new users are to be provided with evidence that the user has read/understood/attested and abide by all applicable policies (upon initial hire and annually thereafter); and
— The CSO is to generate and provide pre-formatted email templates to apply to the scenarios of 'new user', 'modified privilege' user and 'terminated user' for the FOCUS IT Analysts to transmit to applicable users; and
The FOCUS IT Analysts ensure that:
— When registering a new user to have access to the FOCUS RMS, a secure email is transmitted with default credentials which includes text in the email of relevant policies and procedures as applicable to their responsibilities; and
— Confirm authorization (with direct report manager) and confirm minimum access privileges necessary to fulfill the new users' duties prior to granting access; and
— Confirm with direct report manager that access is appropriate to the business and/or clinical needs (consistent with sensitivity/risk and does not violate segregation of duties requirements); and
— When de-registering an existing user from the FOCUS RMS, an email transmitted which includes text in the email of relevant policies and procedures as applicable to their responsibilities reminding the user of their post-access responsibilities (such as originally signed NDA); and
— Clearly indicate in the CSO's pre-formatted email template language as applicable for terminations and transfers; and
— No default accounts may be created; and ensure that default accounts are deleted, if identified; and
— Ensure that privilege sets are synchronized (reduced) in the event an end-user no longer needs higher privilege sets; and
— Ensure that all disabled accounts are removed automatically.

MONITORING:
The FOCUS CSO:
• Monitors training logs and ensure that all users have attested to policies & procedures (initially and annually thereafter); and
• Monitors quarterly meeting minutes and follow up with any required training of FOCUS IT Analysts to ensure compliance; and
• Monitors pre-authored template language that FOCUS IT Analysts will deploy when adding/modifying/deleting users; and
• Monitors random emails sent by the FOCUS IT Analysts for completeness and compliance.

EVIDENCE:
• Company calendar; meeting minutes; training attestations; email samples.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access. Guest/anonymous, shared/group, emergency and temporary accounts are specifically authorized and use monitored. *1110.01b1System.5* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is a policy of FOCUS that guest/anonymous, shared/group, emergency and temporary accounts are prohibited. Evidence shall be the written policy requiring compliance with the elements of this standard; and that **access rights statements** are attested to and on file by each end-user. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
It is a policy of FOCUS that guest/anonymous, shared/group, emergency and temporary accounts are prohibited.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly documented meetings with the FOCUS IT Analysts are scheduled; and
— Training for FOCUS IT Analysts must read/understand/attest and comply with this policy:
- Ensure and document when users are given a written statement of their access rights, which they are required to sign stating they understand the conditions of access.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors training logs to ensure that FOCUS IT Analysts have attested to training on this policy; and
- Monitors end-user inventory logs to ensure that users have signed written statements of their access rights.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; signed access rights.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that covered or critical business information is not left unattended or available for unauthorized individuals to access, including on desks, printers, copiers, fax machines, and computer monitors. *1114.01h1Organizational.123* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Clean Desk Policy v 2.0.pdf**'. Evidence shall be the written policy requiring compliance with the elements of this standard; and that **FOCUS Confidentiality Agreements** are attested to and on file for each end-user; and the **FOCUS Security Policy and Procedure** is attested to and on file for each end-user. Ongoing quality assurance monitoring mechanisms include documented **end-user** annual **training** to ensure that awareness of this FOCUS policy is reiterated. Training events shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection of covered critical business information (e.g., on paper or on electronic storage media) and determine if the information is locked away (ideally in a safe or cabinet or other forms of security furniture) when not required, especially when the office is vacated. Additionally, whether computers and terminals are left logged off or protected with a screen and keyboard locking mechanism controlled by a password, token or similar user authentication mechanism that conceals information previously visible on the display when unattended and are protected by key locks, passwords or other controls when not in use. Documents containing covered or classified information are removed from printers, copiers, and facsimile machines immediately; and when transporting documents with covered information within facilities and through inter-office mail.

PROCEDURES:
— Please refer to the FOCUS policy entitled 'Clean Desk Policy v2.0.pdf'; and
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— All FOCUS Staff Members and contracted Peer Reviewers are to be provided training to read/understand/attest and comply with this policy.

MONITORING:
The FOCUS CSO:
- Monitors the company calendar to ensure policy update compliance; and
- Monitors the training log to ensure that all FOCUS Staff Members and Peer Reviewers comply with the policy.

EVIDENCE:
- Company calendar; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that covered or critical information is protected when using internal or external (e.g., USPS) mail services. *1115.01h1Organizational.45* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is the policy of FOCUS to only deliver protected information via encrypted, secure electronic means as it is prohibited to print and ship any protected information. Evidence shall be the written policy requiring compliance with the elements of this standard; and the **FOCUS Security Policy and Procedure** is attested to and on file for each FOCUS Staff Member and contracted Peer Reviewer. Ongoing quality assurance monitoring mechanisms include documented **end-user** annual **training** to ensure that awareness of this FOCUS policy is reiterated. Training events shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection of covered critical business information and determine if information is not be visible through envelope windows, and envelopes are marked according to its classification level (e.g., confidential). Additionally, incoming and outgoing mail points and unattended facsimile machines are protected.

PROCEDURES:
It is the policy of FOCUS to only deliver protected information via encrypted, secure electronic means as it is prohibited to print and ship any protected information.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to all FOCUS Employees and contracted Peer Reviewers upon hire and annually thereafter that they read/understand/attest and comply with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews; and
- Training logs to ensure that all applicable end users have received and attested to training.

EVIDENCE:
- Company calendar; training attestations

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Strong authentication methods such as multi-factor, Radius or Kerberos and CHAP shall implemented for all external connections to the FOCUS network. *1116.01j1Organizational.145* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure specifying that Two Factor Authentication (TFA) is required for all FOCUS staff members and Peer Reviewers to access the FOCUS Review Management System where PII/PHI is stored; and a screenshot shall be kept on file illustrating the TFA function. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to access control and determine if the authentication of remote users is implemented using a password or passphrase and at least one of the following methods: (i) a cryptographic based technique; (ii) biometric techniques; (iii) hardware tokens; (iv) software tokens; (v) a challenge/response protocol; or, (vi) certificate agents.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The FOCUS CSO establishes documented quarterly meetings to ensure that FOCUS IT Analysts are actively testing to confirm that two-factor authentication is active and functional; and
The FOCUS IT Analysts ensures that:
— Two-factor authentication is required for FOCUS Staff Members and Peer Reviewers to gain access to FOCUS services.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting evidence that two-factor authentication is functional and active.

EVIDENCE:
- Company calendar; training attestations; screenshots of two-factor authentication.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that remote access by vendors and business partners (e.g., for remote maintenance) is disabled/deactivated when not in use. *1117.01j1Organizational.23* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen instructions to remind FOCUS IT Analysts of this requirement. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to remote access and determine if remote access by vendors and business partners (e.g., for remote maintenance) is disabled unless specifically authorized by management. Further, remote access to business partner accounts (e.g., remote maintenance) is immediately deactivated after use.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The FOCUS CSO establishes documented quarterly meetings to ensure that FOCUS IT Analysts are properly disabling/deactivating access to vendors and business partners when access is not needed; and
The FOCUS IT Analysts ensures that:
— FOCUS IT Analysts are properly disabling/deactivating access to vendors and business partners when access is not needed.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting evidence that proper disabling/deactivating access to vendors and business partners is occurring when access is not needed.

EVIDENCE:
- Company calendar; training attestations; screenshots of disabled accounts.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
Unique IDs that can be used to trace activities to the responsible individual are required for all types of FOCUS and non-FOCUS users. *1122.01q1System.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen non-editable unique user IDs which are incorporated into audit logs for tracing accountability. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine if before allowing access to system components or data, the organization requires verifiable unique ID's for all types of users including, but not limited to: technical support personnel, operators, network administrators, system programmers, and database administrators.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The FOCUS CSO establishes documented quarterly meetings to ensure that FOCUS IT Analysts are ensuring that unique IDs are assigned to each user for the purpose of tracing activities of all users of the RMS system; and
The FOCUS IT Analysts ensure that:
— FOCUS IT Analysts are properly ensuring that unique IDs are assigned to each user for the purpose of tracing activities of all users of the RMS system.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting evidence that documents properly ensuring that unique IDs are assigned to each user for the purpose of tracing activities of all users of the RMS system.

EVIDENCE:
- Company calendar; training attestations; screenshots of sample ID numbers.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that users who performed privileged functions (e.g., system administration) use separate accounts when performing those privileged functions. *1123.01q1System.2* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen non-editable unique user IDs as well as unique privilege sets which provide for privileged functions which are incorporated into audit logs for tracing accountability. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine whether user IDs are used to trace activities to the responsible individual and regular user activities are not performed from privileged accounts.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO and FOCUS IT Analysts are to use personalized, secondary accounts when performing high-level administrative functions; and
— The FOCUS CSO establishes quarterly meetings to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that shared/group and generic user IDs are only used in exceptional circumstances where there is a clear business benefit, when user functions do not need to be traced, additional accountability controls are implemented, and after approval by management. *1124.01q1System.34* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is FOCUS policy that shared/group accounts and generic user IDs are prohibited at all times. Evidence of meeting this standard includes the policy/procedure; and a **screenshot** of the user account function with on-screen options which do not include shared/group or generic user IDs. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine whether shared user/group IDs are only used in exceptional circumstances, where there is a clear business benefit, the use of a shared user ID for a group of users or a specific job can be used, approval by management is documented for such cases, and additional controls are required to maintain accountability. Further, determine if generic IDs that are used by an individuals are allowed either where the functions accessible or actions carried out by the ID do not need to be traced (e.g., read only access).

PROCEDURES:
It is FOCUS policy that shared/group accounts and generic user IDs are prohibited at all times.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that at no time shared/group or generic user IDs are created for any user; and
— The FOCUS CSO establishes quarterly meetings to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that access rights to applications and application functions are limited to the minimum necessary using menus. *1129.01v1System.12* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management.. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the RMS user account function illustrating minimum menu functions for all end-users, as all required processes are presented on the user interface (UI) of the RMS without the need of menus. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts on a quarterly basis to ensure that the on-screen function and selection options meet this FOCUS policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO is to provide training to the FOCUS IT Analysts to ensure that only minimum menu items are required as the RMS UI must provide all functions in pre-programmed buttons; and
— The FOCUS CSO establishes quarterly meetings to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitor:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Upon termination or changes in employment for employees, contractors, third-party users or other workforce arrangement, FOCUS shall ensure that physical and logical access rights and associated materials (e.g., passwords, keycards, keys, documentation that identify them as current members of FOCUS) are removed or modified to restrict access within 24 hours and old accounts are closed after 90 days of opening new accounts. *1135.02i1Organizational.1234* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy/procedure supporting this standard within the specified hours/days; and a **screenshot** of the user account function with on-screen buttons for use when a FOCUS staff member, Peer Reviewer or Client-Company end-user relationship to FOCUS changes. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to removal of access rights and determine whether the organization upon termination, the access rights for the terminated individual is disabled in a timely manner, at least within 24 hours. Further, changes of employment or other workforce arrangement (e.g., transfers) is reflected in removal of all access rights that were not approved for the new employment or workforce arrangement. Access changes due to personnel transfer are managed effectively. Old accounts are closed after 90 days, and new accounts opened. The access rights is removed or adapted include physical and logical access, keys, identification cards, IT systems and application, subscriptions, and removal from any documentation that identifies them as a current member of the organization. If a departing employee, contractor, third-party user or other workforce member has known passwords for accounts remaining active, these are changed upon termination or change of employment, contract, agreement, or other workforce arrangement.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The FOCUS CSO establishes documented quarterly meetings to ensure that FOCUS IT Analysts are properly disabling/deactivating access to end users per the above policy when access is not appropriate; and
The FOCUS IT Analysts ensure that:
— FOCUS IT Analysts are properly disabling/deactivating access to end users when access is inappropriate.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting evidence that proper disabling/deactivating access when access is inappropriate.

EVIDENCE:
- Company calendar; training attestations; screenshots of disabled accounts.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that acceptable use agreements are signed by all employees before being allowed access to information assets. *1137.06e1Organizational.1* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Terms of Use v2.0.pdf**'. Evidence of meeting this standard includes the policy/procedure supporting this standard; and initial and annual attestation to the **FOCUS Acceptable Use Agreement** shall be on file for each FOCUS staff member and Peer Reviewer. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts on a quarterly basis to ensure that attestations are on file for all FOCUS Staff Members and Peer Reviewers. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to prevention of misuse of information to determine if communication to all employees has notified them that their actions may be monitored and that, through signing an acceptable use agreement, they have consented to such monitoring (Note: the legality of such monitoring must be verified in each legal jurisdiction).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to all FOCUS Staff Members upon hire that they read/understand/attest and comply with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of file reviews to confirm attestations by all FOCUS Staff Members are to be documented.

EVIDENCE:
- Company calendar; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that user access rights are reviewed after any changes and reallocated as necessary. *1166.01e1System.12* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy/ procedure supporting this standard. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to review user access right change reports to confirm compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to system account management and determine if user's access rights are reviewed after any changes, such as promotion, demotion, or termination of employment, or other arrangement with a workforce member ends. Further, access rights are reviewed and re-allocated when moving from one employment or workforce member arrangement to another within the same organization.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are directed to notify the CSO upon each and every access privilege modification; and
— Training is to be provided regarding this policy to all FOCUS IT Analysts upon hire and annually thereafter that they read/understand/ attest and comply with this policy; and
— Per user access right modification request, the CSO reviews changes and confirm accuracy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of user access rights to confirm accuracy.

EVIDENCE:
- Company calendar; training attestations; user access right samples.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that a time-out system (e.g. a screen saver) pauses the session screen after 15 minutes of inactivity, closes network sessions after 30 minutes of inactivity, and requires the user to reestablish authenticated access once the session has been paused or closed; or, if the system cannot be modified, a limited form of time-out that clears the screen but does not close down the application or network sessions is used. *11126.01t1Organizational.12* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a series of screenshots depicting the time and actions of the system requiring reestablishment of authentication for FOCUS Staff Members and Peer Reviewers. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to review testing to confirm compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are directed to ensure that all FOCUS Employee systems provide the time-out as specified above; and
— FOCUS IT Analysts are directed to ensure that all web users (client-companies and contract Peer Reviewers) times out user sessions as specified in the policy above; and
— Training is to be provided regarding this policy to all FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The CSO schedules a quarterly meeting with FOCUS IT Analysts to confirm implementation and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of timeout settings to confirm accuracy.

EVIDENCE:
- Company calendar; training attestations; screenshots of timeout settings.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that bring your own device (BYOD) and/or company-owned devices are configured to require an automatic lockout screen, and the requirement is enforced through technical controls. *11190.01t1Organizational.3* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a series of screenshots depicting the time and actions of the system automatically initiating a lockout screen for FOCUS Staff Members and Peer Reviewers. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to review testing to confirm compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that employees must be provided FOCUS owned and managed devices and that remote management tools must be installed.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are directed to configure devices to require an automatic lockout screen with remote management tools; and
— Training is to be provided regarding this policy to all FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm implementation and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of lockout settings to confirm accuracy.

EVIDENCE:
- Company calendar; training attestations; screenshots of lockout settings.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that privileges are formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element. *1143.01c1System.123* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen authorization by a FOCUS manager for the initial or modified privileges per FOCUS staff member, Peer Reviewer or Client-Company end-user. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to all FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— Each end-user privilege set has been formally authorized and controlled, allocated to users on a need-to-use and event-by-event basis for their functional role (e.g., user or administrator), and documented for each system product/element.
— The CSO schedules a quarterly meeting with FOCUS IT Analysts to confirm implementation and review system settings.
The FOCUS IT Analysts ensures that:
— Upon receiving instructions from the CSO, allocation of each end users' privilege set is to be accurately assigned.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of privileges to confirm accuracy.

EVIDENCE:
- Company calendar; training attestations; screenshots of privilege sets.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall explicitly authorize access to specific security relevant functions (deployed in hardware, software, and firmware) and security-relevant information. *1144.01c1System.4* These requirements are stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen authorization of security functions by a FOCUS manager for the FOCUS staff member. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to privilege management and determine if at a minimum, the organization explicitly authorizes access to the following list of security functions (deployed in hardware, software, and firmware) and security-relevant information: (i) Setting/modifying audit logs and auditing behavior; (ii) Setting/modifying boundary protection system rules; (iii) Configuring/modifying access authorizations (e.g., permissions, privileges); (vi) Setting/modifying authentication parameters; and, (v) Setting/modifying system configurations and parameters.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding explicit authorizations per Analyst to all FOCUS IT Analysts upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— Each FOCUS IT Analyst is to be given, in writing, explicit authorization to allow administrative responsibility and access deployed in hardware, software, and firmware to manage these assets; and
— The CSO schedules a quarterly meeting with FOCUS IT Analysts to review authorizations and confirm authenticity.
The FOCUS IT Analysts ensure that:
— Upon receiving explicit authorizations from the CSO, they must maintain these authorization notifications for their respective records.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Quarterly meeting minutes of authorizations to confirm accuracy.

EVIDENCE:
- Company calendar; training attestations; examples of authorizations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:

FOCUS shall ensure that access to network equipment is physically protected. *1192.01I1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Access to and securing of Network Equipment**'. Evidence of meeting this standard includes the policy/ procedure supporting this standard; and signed attestation to the FOCUS Confidentiality Agreement (upon initial hire and annually thereafter); and signed attestation to the FOCUS Security Policy and Procedure (upon initial hire and annually thereafter). Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts recorded on a quarterly basis to ensure that this FOCUS policy is being properly executed; and that all network equipment is inventoried and accounted for. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:

The FOCUS CSO ensures that:

— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS data center(s), where all FOCUS networking resides, is housed in a locked cabinet; and
— Each data center has security elements in place to ensure that only authorized personnel have access to cabinet(s); and
— The CSO schedules a quarterly meeting with FOCUS Data center providers to review authorized personnel records and confirm appropriateness.

MONITORING:

The FOCUS CSO monitors:

- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Data center access logs to ensure that only authorized personnel have access to cabinets; and
- Quarterly meeting minutes to document and confirm accuracy.

EVIDENCE:

- Company calendar; meeting minutes; Data Center authorized personnel list.

POLICY:
FOCUS shall ensure that account types are identified (individual, shared/group, system, application, guest/anonymous, emergency and temporary), conditions for group and role membership are established, and, if used, shared/group account credentials are modified when users are removed from the group. *1139.01b1System.68* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy/procedure supporting this standard; and a **screenshot** of the user account function with on-screen authorization of categorization of the FOCUS staff member as *individual, shared/group, system, application, guest/anonymous, emergency and temporary*. Ongoing quality assurance monitoring mechanisms include documented **meeting minutes** the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that this FOCUS policy is being properly executed; with review and verification of accuracy regarding each user and their assigned account types. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that shared/group accounts and guest/anonymous accounts and emergency and temporary accounts are prohibited at all times.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that at no time shared/group or guest/anonymous accounts and emergency and temporary accounts are created for any user; and
— The FOCUS CSO establishes quarterly meetings to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that if encryption is not used for dial-up connections, the CSO or his/her designated representative provides specific written authorization *1173.01j1Organizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is FOCUS policy that dialup connections to the FOCUS network are prohibited. Evidence of meeting this standard includes the policy/procedure supporting this standard through prohibition of analog dial-up access to FOCUS systems; and training with signed attestations to the FOCUS Security Policy and Procedure by each FOCUS Staff Member and Peer Reviewer upon initial hire and annually thereafter. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that this FOCUS policy is being properly executed; with review and verification of accuracy regarding each user and their assigned account types. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
It is FOCUS policy that dialup connections to the FOCUS network are prohibited.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that at no time does FOCUS allow dial-up connections to the FOCUS network; and
— The FOCUS CSO establishes quarterly meetings to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall protect wireless access to systems containing sensitive information by authenticating both users and devices. *1174.01j1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard through prohibition of wireless access points provided by FOCUS; and training with signed attestations to the FOCUS Security Policy and Procedure by each FOCUS IT Staff Member upon initial hire and annually thereafter. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that this FOCUS policy is being properly executed. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS that WiFi is not provided by FOCUS IT and use of WiFi by FOCUS Staff Members is prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that at no time are WiFi (wireless) networks to be configured for use on the FOCUS network; and
— The FOCUS CSO provides training to FOCUS Staff Members to ensure that at no time are WiFi (wireless) access to be utilized when connecting to the FOCUS network; and
— The FOCUS CSO establishes quarterly meetings with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance; and
- FOCUS Staff Member attestations in the training log.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that remote access to business information across public networks only takes place after successful identification and authentication. *1175.01j1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; and requirement of all FOCUS Staff Members and Peer Reviewers are subject to two-factor authentication (TFA) when authenticating; and training with signed attestations to the FOCUS Security Policy and Procedure by each FOCUS Staff Member and Peer Reviewer upon initial hire and annually thereafter. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that all FOCUS Staff Members and Peer Reviewers are actively utilizing TFA based on reports generated by the Review Management System. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provide straining to the FOCUS IT Analysts to ensure that remote access to business information across public networks only takes place after successful identification and authentication; and
— The FOCUS CSO establishes quarterly meetings with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance; and
- FOCUS IT Analyst attestations in the training log.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that redundant user IDs are not issued to other users and that all users are uniquely identified and authenticated for both local and remote access to information systems. *11109.01q1Organizational.57* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; and requirement of all FOCUS Review Management System users must have unique user IDs; and a **screenshot** of the account creation function within the FOCUS Review Management System illustrating an error dialog if a User ID already exists when attempting to add a new user, preventing duplication; and training with signed attestations to the FOCUS Security Policy and Procedure by each FOCUS Staff Member and Peer Reviewer upon initial hire and annually thereafter; and that this standard is stipulated in the **FOCUS Terms of Use** documentation available to all users. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that all users of the FOCUS Review Management System are assigned unique User IDs, based on reports generated by the Review Management System. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that redundant user IDs are not issued to other users and that all users are uniquely identified and authenticated for both local and remote access to information systems; and
— The FOCUS CSO establishes quarterly meetings with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance; and
- FOCUS IT Analyst attestations in the training log.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that Non-FOCUS users (all information system users other than FOCUS users, such as patients, customers, contractors, or foreign nationals), or processes acting on behalf of non-FOCUS users, determined to need access to information residing on FOCUS's information systems, are uniquely identified and authenticated. *11110.01q1Organizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; and requirement of all FOCUS Review Management System users must have unique user IDs; and a **screenshot** of the account creation function within the FOCUS Review Management System illustrating an error dialog if a User ID already exists when attempting to add a new user, preventing duplication; and that this standard is stipulated in the **FOCUS Terms of Use** documentation available to all users. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to ensure that all users of the FOCUS Review Management System are assigned unique User IDs, based on reports generated by the Review Management System. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS that only FOCUS Employees, client-company personnel and contracted Peer Reviewers or authorized automated servers (APIs) are allowed to access the FOCUS network.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that only FOCUS Employees, client-company personnel and contracted Peer Reviewers, authorized vendors or authorized automated servers (APIs) are allowed to access the FOCUS network; and
— All authorized users must have a unique authentication identifier; and
— The FOCUS CSO establishes quarterly meetings with FOCUS IT Analysts to review and confirm compliance with this policy.
— Please refer to FOCUS Policy entitled '**Review Control Policy**' for RMS field-level controls defining which user groups are eligible to *create, edit, modify,* or *read only* during each process step during the lifecycle of a Peer Review.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance; and
- FOCUS IT Analyst attestations in the training log.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors. *11154.02i1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy and procedure supporting this standard; and policy requirement that FOCUS administration notify the CSO of employee position modifications or termination occurs; and a **screenshot** of the account creation function within the FOCUS Review Management System illustrating the ability to suspend or terminate a User Account; and that this standard is stipulated in the **FOCUS Terms of Use** documentation available to all users. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System indicating which users are active, suspended or terminated. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to removal of access rights and determine whether access rights to information assets and facilities are reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors including: (i) whether the termination or change is initiated by the employee, contractor, third-party user, other workforce member, or by management and the reason of termination; (ii) the current responsibilities of the employee, contractor, workforce member or any other user; and, (iii) the value of the assets currently accessible.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts to ensure that access rights to information assets and facilities is reduced or removed before the employment or other workforce arrangement terminates or changes, depending on the evaluation of risk factors; and
— The FOCUS CSO provides clear instructions to the FOCUS IT Analysts before access rights are altered or terminated; and
— The FOCUS CSO establishes quarterly meetings with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance; and
- FOCUS IT Analyst attestations in the training log.

EVIDENCE:
- Company calendar; meeting minutes; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall require that electronic signatures, unique to one individual, cannot be reused by, or reassigned to, anyone else. *11208.01q1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to visually ensure that all electronic signatures are unique. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS that electronic signatures are prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— In the event this policy must be modified to provide electronic signatures, the policy will be modified to securely address electronic signatures prior to implementation.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Meeting minutes to review minutes and confirm compliance.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain a current listing of all workforce members (individuals, contractors and Business Associates) with access to PHI. *11219.01b1Organizational.10* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; and **User Account Reports** that are generated and stored within the FOCUS Review Management System Administration Screen; and a **screenshot** of the RMS Administration Screen showing the inventory of reports. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS RMS system requires entry of all authorized workforce members; and
— Reports are generated quarterly and reviewed by the CSO for compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Reports generated by the RMS on a quarterly basis.

EVIDENCE:
- Company calendar; workforce member reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that user registration and de-registration formally address establishing, activating, modifying, reviewing, disabling and removing accounts. *11220.01b1System.10* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard which stipulates that all new user accounts must be screened and established by FOCUS IT Analysts; and history of registration/de-registration/activating/modifying/reviewing/disabling and removing accounts is recorded; and that **User Account Reports** are generated and stored within the FOCUS Review Management System Administration Screen; and a **screenshot** of the RMS Administration Screen showing the inventory of reports. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user account administration and determine if user registration and de-registration formally addresses establishing, activating, modifying, reviewing, disabling and removing accounts. Further, at a minimum, the organization addresses how access requests to information systems are submitted, how access to the information systems is granted, how requests to access covered information are submitted, how access to covered information is granted, how authorization and/or supervisory approvals are verified, and how a workforce members level of access to covered information is verified.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts that all new user accounts must be screened and established by FOCUS IT Analysts; and history of registration/de-registration/activating/modifying/reviewing/disabling and removing accounts is recorded; and
— Reports are generated quarterly and reviewed by the CSO for compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Reports generated by the RMS on a quarterly basis.

EVIDENCE:
- Company calendar; workforce member reports; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that group, shared or generic accounts and passwords (e.g., for first-time log-on) are not used. *1111.01b2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is FOCUS policy that group, shared or generic accounts and passwords are prohibited. Evidence of meeting this standard includes the policy and procedure supporting this standard which prohibits the use of group, shared or generic accounts and passwords; and a screenshot with instructions on the User Account function within the Review Management System which prohibits creation of group, shared or generic accounts and passwords. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CSO provides training to the FOCUS IT Analysts that group, shared or generic accounts and passwords (e.g., for first-time log-on) are not used; and
— Reports are generated quarterly and reviewed by the CSO for compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Reports generated by the RMS on a quarterly basis.

EVIDENCE:
- Company calendar; workforce member reports; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that user identities are verified in person before a designated registration authority with authorization by a designated FOCUS official (e.g., a supervisor or other individual defined in an applicable security plan) prior to receiving a hardware token. *1112.01b2System.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard which requires **in-person identity verification** for FOCUS Staff Members prior to activating their User Account; and a placeholder for the front and back of each FOCUS Staff Member **driver's license image** with photo; and a **screenshot** with instructions on the User Account function within the Review Management System which requires in-person identity verification. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate. All annual and monitoring activities is to be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CEO, CMO, CSO, CSO or CFO is to verify the identity of any new Employee or contracted Peer Reviewer prior to allowing access to FOCUS systems; and
— Provide training to the CEO, CMO, CSO, CSO to ensure that proper measures are taken, including evidence gathering measures, while meeting in person with the new Employee or contracted Peer Reviewer; and
— That no individual is provided access to FOCUS systems until evidence gathered is entered into the RMS and verified by the CSO; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Employee and contracted Peer Reviewer logs, collected identification data and authorizations.

EVIDENCE:
- Company calendar; Employee and contracted Peer Reviewer logs; training attestations; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that multi-factor authentication methods are used in accordance with organizational policy, (e.g., for remote network access). *1125.01q2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the requirement that all FOCUS Staff Members and Peer Reviewers may only access the FOCUS Review Management System after providing their Account Name, Password and 4-digit PIN that they receive as a SMS text message on their mobile phone each time they attempt to login; and a series of **screenshot**s illustrating the two-factor authentication process. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that all users are actively utilizing two factor authentication. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine if appropriate authentication methods including strong authentication methods in addition to passwords are used for communicating through an external, non-organization-controlled network (e.g., the Internet).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided to the FOCUS IT Analysts on training end-users of its required continual operation and periodic testing; and
The FOCUS IT Analysts ensure that:
— Evidence is gathered that each FOCUS Staff Member and contracted Peer Reviewer is required to utilize two-factor authentication; and
— Logs record evidence that two-factor authentication is utilized for each login session.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Employee and contracted Peer Reviewer log evidence showing compliance with this policy.

EVIDENCE:
- Company calendar; Employee and contracted Peer Reviewer logs; training attestations.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that where tokens are provided for multi-factor authentication, in-person verification is required prior to granting access. *1127.01q2System.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard which requires **in-person identity verification** for FOCUS Staff Members prior to activating their User Account and prior to being given a token, if applicable; and a placeholder for the front and back of each FOCUS Staff Member **driver's license image** with photo; and a **screenshot** with instructions on the User Account function within the Review Management System which requires in-person identity verification. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine if during the registration process to provide new or replacement hardware tokens, in-person verification is required in front of a designated registration authority with authorization by a designated organizational official (e.g., a supervisor).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS CEO, CMO, CSO, CSO or CFO is to verify the identity of any new Employee or contracted Peer Reviewer prior to allowing access to FOCUS systems; and
— Provide training to the CEO, CMO, CSO, CSO to ensure that proper measures are taken, including evidence gathering measures, while meeting in person with the new Employee or contracted Peer Reviewer; and
— That no individual is provided access to FOCUS systems until evidence gathered is entered into the RMS and verified by the CSO; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Employee and contracted Peer Reviewer logs, collected identification data and authorizations.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS help desk support shall require user identification for any transaction that has information security implications. *1128.01q2System.5*
This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard which requires **4-digit PIN codes** assigned to all users of the FOCUS Review Management System; and addition of this PIN code to the **FOCUS Onboarding Policy and Procedure**. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review reports generated by the Review Management System to ensure that the reports are current and accurate, and that each user has a unique PIN code. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is provided to the FOCUS IT Analysts to ensure that proper measures are taken to identify incoming requests for assistance by:
  • Confirming the name, phone number and email addresses on file for the requestor; and
  • Requiring the requestor to provide the pre-determined 4-digit support PIN (personal identification number) before assisting the requestor; and
— No individual is to be provided assistance without the above information being confirmed; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
• The company calendar to ensure compliance for policy reviews and quarterly meetings; and
• Employee and contracted Peer Reviewer logs, collected identification data and authorizations.

EVIDENCE:
• Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
• FOCUS IT Analyst

POLICY:
FOCUS shall ensure that access rights from an application to other applications are controlled. *1130.01v2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard which indicates that because FOCUS only utilizes one central data system, access rights are controlled within the FOCUS Review Management System and no further management of access rights are required. Ongoing quality assurance includes the FOCUS CSO and FOCUS IT Analysts record **meeting minutes** on a quarterly basis to maintain awareness of this policy and confirm that access rights are singularly managed within the single source of PII/PHI within the company. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information access restriction and determine whether access rights to other applications are controlled according to applicable access control policies.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that access rights from an application to other applications are controlled; and
— As of the effective date of this policy, FOCUS has but one centralized all-encompassing application, with no need to pass access rights from application to application; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations. *1131.01v2System.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System User Interface (UI) provides only the minimum necessary information for a FOCUS Staff Member or Peer Reviewer to conduct their function; and that **downloading of data** is prevented and prohibited; and a **screenshot** of the account creation function in the FOCUS Review Management System illustrating user privileges; and **attestations** from all FOCUS Staff Member and Peer Reviewers of the **FOCUS Confidentiality Agreement** and **FOCUS Security Policy and Procedure** regarding protection mechanisms prohibiting the accessing/downloading/printing of PII/PHI data. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information access restriction and determine whether the organization ensures that outputs from application systems handling covered information contain only the information relevant to the use of the output and are sent only to authorized terminals and locations.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that outputs from application systems handling covered information are limited to the minimum necessary and sent only to authorized terminals/locations based on privilege sets; and
— As of the effective date of this policy, FOCUS established privilege sets govern the available functions regarding access rights on a per-user basis to prevent unintended release of covered information; and
— FOCUS Prohibits the printing, screen-shooting (generation of screenshots), manually written notes or any other method of extracting PHI/PII from the FOCUS Review Management System for any reason; and
— FOCUS IT Prevents printing of all screens within the FOCUS Review Management System with 'Hide when Printing' setting; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that covered information is encrypted when stored in non-secure areas and, if not encrypted at rest, the FOCUS CSO shall document its rationale. *1132.01v2System.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System User Interface (UI) provides all storage and presentation of appropriate, limited exposure of PII/PHI for FOCUS Staff Members and Peer Reviewers to access to conduct their function; and that **downloading and printing of data** is both prevented and prohibited. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information access restriction and determine whether data stored in information systems is protected with system access controls, including file system, network share, claims, application, and/or database specific access control lists, is encrypted when residing in non-secure areas. Periodic reviews of such output are performed to ensure that redundant information is removed.

NOTE: It is FOCUS policy that at no time shall covered information be stored in non-secure areas.

PROCEDURES:
The FOCUS CSO ensurse that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that exporting or printing by FOCUS Employees or contracted Peer Reviewers is prevented and prohibited; and
— It is prohibited to allow covered information to be stored in non-secure areas.
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that actions that can be performed without identification and authentication are permitted by exception. *1133.01v2System.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System requires all users to have a unique User ID, and that the system has an integrated auditing tool to track all actions taken by any and all users based on their unique User ID; and a screenshot of the Account Creation Function illustrating the unique User ID for each user. Ongoing quality assurance includes the FOCUS CSO record **meeting minutes** on a quarterly basis to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information access restriction and determine whether actions to be performed without identification and authentication are permitted only to the extent necessary to accomplish mission objectives.

NOTE: It is the policy of FOCUS that identification and authentication is required for all hardware/software/maintenance/systems work.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that actions that can be performed without identification and authentication are not permitted; and
— Quarterly documented meetings shall be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that role-based access control is implemented and capable of mapping each user to one or more roles, and each role to one or more system functions. *1145.01c2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System Account Creation Function provides on-screen indicators when a privilege set is assigned to a user so that confirmation of the user's exposure to PII/PHI is the least necessary to perform their function; and a **screenshot** of the Account Creation Function illustrating the on-screen indicators of the user's role(s). Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, the RMS User Inventory Report to review privileges and roles for accuracy; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that role-based access control is implemented and capable of mapping each user to one or more roles, and each role to one or more system functions; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes; account creation and privilege set assignments.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall promote the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users. *1146.01c2System.23* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas FOCUS IT Analyst software development shall not include the use of automated or end-user privilege elevation to accommodate automation; and **attestations** by the FOCUS IT Analysts initially and annually of the FOCUS Security Policy and Procedure. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, all automation software developed within the RMS to ensure that privileges are not elevated for this purpose; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that FOCUS promotes the development and use of programs that avoid the need to run with elevated privileges and system routines to avoid the need to grant privileges to users; and
— At the time of this policy effective date, FOCUS only utilizes one (1) system, thereby not requiring the 'passing' of existing privileges nor expanding privileges for users to access subsequent programs, thereby reducing security; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes; account creation and privilege set assignments.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that elevated privileges are assigned to a different user ID from those used for normal business use, all users access privileged services in a single role, and such privileged access is minimized. *1147.01c2System.456* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes prohibition of any user being assigned multiple accounts within the FOCUS Review Management system; and **attestations** by FOCUS Staff Members and Peer Reviewers initially and annually thereafter. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, the User Access Report to ensure that no individual has more than one login; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that elevated privileges are assigned to a different user ID from those used for normal business use, all users access privileged services in a single role, and such privileged access is minimized; and
— Training is provided to any applicable FOCUS Staff Members directing those with elevated privileges to use the different User ID so as to maximize security; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes; account creation and privilege set assignments.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall restrict access to privileged functions and all security-relevant information. *1148.01c2System.78* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS CSO must approve any and all users with high level privileged functions to access privileged functions and all sensitive security-relevant information; and **attestations** by the FOCUS Management Staff of the FOCUS Confidentiality Agreement and FOCUS Security Policy and Procedure initially and annually thereafter. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, the User Access Report to ensure that no inappropriate individual has privileged functions nor access to sensitive security-relevant information; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to privilege management and determine if access to privileged functions (e.g., system-level software, administrator tools, scripts, utilities) deployed in hardware, software, and firmware is restricted and access to security relevant information is be restricted to explicitly authorized individuals.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that FOCUS restricts access to privileged functions and all security-relevant information; and
— Training is provided to any applicable FOCUS Staff Members directing those with elevated privileges to use the different User ID so as to maximize security; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes; account creation and privilege set assignments.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall facilitate information sharing by enabling authorized users to determine a business partner's access when discretion is allowed as defined by FOCUS and by employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions. *1149.01c2System.9* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure stipulating that the FOCUS CSO approving any advanced access to information beyond the current, restricted user interface access to PII/PHI; and **attestations** by the FOCUS Management Staff of the FOCUS Confidentiality Agreement and FOCUS Security Policy and Procedure initially and annually thereafter. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, the User Access and Privileges within the RMS to ensure that privileges of users and functions available to them protect sensitive information; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information sharing and determine if the organization facilitates information sharing by: (i) enabling authorized users to determine whether access authorizations assigned to business partners match the access restrictions on information for specific circumstances in which user discretion is allowed; and, (ii) employing manual processes or automated mechanisms to assist users in making information sharing/collaboration decisions.

NOTE: it is FOCUS policy that the FOCUS CSO shall evaluate all requests of information sharing outside of established norms so as to ensure security of covered information.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that the FOCUS CSO is to evaluate, approve (or deny) all requests of information sharing outside of established norms so as to ensure security of covered information for the duration of the need; and
— Training is provided to any applicable FOCUS Staff Members directing those with elevated privileges to submit requests for such needs to CSO; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the access control system for the system components storing, processing or transmitting covered information is set with a default "deny-all" setting. *1150.01c2System.10* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the default account settings default to 'deny-all'; and a **screenshot** of the default user setting visually indicating this. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, the default account settings to ensure that access is set to 'deny-all' by default; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that FOCUS access control systems that store, process or transmit covered information is set with a default "deny-all" setting.
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that when PKI-based authentication is used, the information system validates certificates by constructing and verifying a certification path to an accepted trust anchor, including checking certificate status information; enforces access to the corresponding private key; maps the identity to the corresponding account of the individual or group; and implements a local cache of revocation data to support path discovery and validation in case of an inability to access revocation information via the network. *11111.01q2System.4* This requirement has been deemed not applicable to FOCUS, as PKI-based authentication is not implemented within FOCUS. However, in the event PKI-based authorization is implemented, FOCUS shall generate the policy and procedural requirements to support this HITRUST standard.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews.

EVIDENCE:
- Company calendar; annual meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the information system employs replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps to secure network access for privileged accounts; and, for hardware token-based authentication, employs mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline. *11112.01q2Organizational.67* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**User Accounts**'. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the use of unique 4-digit PIN numbers per login attempt during the Two-Factor Authentication (TFA) process is set to NULL after the successful login; therefore repeated attempts to login with the combination of user name, password and PIN will not be successful; and a **screenshot** of this PIN nullification upon successful login to ensure compliance. Ongoing quality assurance includes the FOCUS CSO shall review, on a quarterly basis, confirmation that TFA PINS are indeed nullified after each successful login; and to record **meeting minutes** to review this policy and ensure compliance. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Quarterly meetings are held with the FOCUS IT Analysts to confirm compliance with this policy; and
— Training is provided to the FOCUS IT Analysts to ensure that the FOCUS RMS system employs replay-resistant authentication mechanisms such as nonce, one-time passwords, or time stamps to secure network access for privileged accounts; and
— For hardware token-based authentication (if/when deployed by FOCUS), employs mechanisms that satisfy minimum token requirements discussed in NIST SP 800-63-2, Electronic Authentication Guideline; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that identity verification of the individual is required prior to establishing, assigning, or certifying an individual's electronic signature or any element of such signature. *11200.01b2Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This requirement has been deemed not applicable to FOCUS, as electronic signature technologies are not implemented within the company. However, in the event electronic signature technologies are implemented, FOCUS shall generate the policy and procedural requirements to support this HITRUST standard.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews.

EVIDENCE:
- Company calendar; annual meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that electronic signatures based upon biometrics are designed to ensure that they cannot be used by any individual other than their genuine owners. *11209.01q2Organizational.9* This requirement has been deemed not applicable to FOCUS, as biometric based signatures are not implemented within the company. However, in the event biometric based signatures are implemented, FOCUS shall generate the policy and procedural requirements to support this HITRUST standard.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews.

EVIDENCE:
- Company calendar; annual meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that electronic signatures and handwritten signatures executed to electronic records are linked to their respective electronic records. *11210.01q2Organizational.10* This requirement has been deemed not applicable to FOCUS, as biometric based signatures are not implemented within the company. However, in the event biometric based signatures are implemented, FOCUS shall generate the policy and procedural requirements to support this HITRUST standard.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews.

EVIDENCE:
- Company calendar; annual meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensures that signed electronic records contain information associated with the signing in human-readable format. *11211.01q2Organizational.11* This requirement has been deemed not applicable to FOCUS, as biometric based signatures are not implemented within the company. However, in the event biometric based signatures are implemented, FOCUS shall generate the policy and procedural requirements to support this HITRUST standard.

FOCUS shall examine policies and/or standards related to user identification and authentication and determine if signed electronic records contain information associated with the signing that clearly indicates the following in human-readable format: (i) printed name of the signer; (ii) the date and time when the signature was executed; and, (iii) the meaning of the signature (e.g., review, approval, responsibility, authorship).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews.

EVIDENCE:
- Company calendar; annual meeting minutes.

POLICY:
FOCUS shall ensure that copy (including print screen), move, print, and storage of sensitive data are prohibited when accessed remotely without a defined business need. *1134.01v3System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is FOCUS policy that copying, moving, printing or storing of sensitive data outside of the provided RMS environment is prohibited. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas screenshots, printing of any type, moving of data and storage of sensitive data on FOCUS Staff Member's local or remote systems is strictly prohibited; and a **screenshot** of the remote system desktop image which reiterates this policy; and a screenshot of computer system management software disabling printing, copying and pasting of sensitive data between remote systems and the local system a user accesses. Ongoing quality assurance includes a review by the CSO, on a quarterly basis, the System Administrative software to ensure settings are active to prevent screenshots, moving, printing or storage of any sensitive data; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information access restriction and determine if individuals accessing sensitive information (e.g., covered information, cardholder data) from a remote location, then the copy, move, print (and print screen) and storage of this information onto local hard drives and removable electronic media is prohibited, unless explicitly authorized for a defined business need.

PROCEDURES:
It is FOCUS policy that copying, moving, printing or storing of sensitive data outside of the provided RMS environment is prohibited. The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Documented quarterly meetings are held to confirm compliance with this policy; and
— Training is provided to all FOCUS Staff Members and IT Analysts to ensure that copying, moving, printing or storing of sensitive data outside of the provided RMS environment is prohibited; and
— Quarterly documented meetings are to be held with FOCUS IT Analysts to review and confirm compliance with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Quarterly meeting minutes held with FOCUS IT Analysts to confirm compliance with this policy.

EVIDENCE:
- Company calendar; training attestations, meeting minutes; screenshots of on-screen notices of prohibition.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

1106.01b1System.1	HITRUST 01.b User Registration
1107.01b1System.2	HITRUST 01.b User Registration
1108.01b1System.3	HITRUST 01.b User Registration
1109.01b1System.479	HITRUST 01.b User Registration
1110.01b1System.5	HITRUST 01.b User Registration
1114.01h1Organizational.123	HITRUST 01.h Clear Desk and Clear Screen Policy
1115.01h1Organizational.45	HITRUST 01.h Clear Desk and Clear Screen Policy
1116.01j1Organizational.145	HITRUST 01.j User Authentication for External Connections
1117.01j1Organizational.23	HITRUST 01.j User Authentication for External Connections
1122.01q1System.1	HITRUST 01.q User Identification and Authentication
1123.01q1System.2	HITRUST 01.q User Identification and Authentication
1124.01q1System.34	HITRUST 01.q User Identification and Authentication
1129.01v1System.12	HITRUST 01.v Information Access Restriction
1135.02i1Organizational.1234	HITRUST 02.i Removal of Access Rights
1137.06e1Organizational.1	HITRUST 06.e Prevention of Misuse of Information Assets
1166.01e1System.12	HITRUST 01.e Review of User Access Rights
11126.01t1Organizational.12	HITRUST 01.t Session Time-out
11190.01t1Organizational.3	HITRUST 01.t Session Time-out
1143.01c1System.123	HITRUST 01.c Privilege Management
1144.01c1System.4	HITRUST 01.c Privilege Management
1192.01l1Organizational.1	HITRUST 01.l Remote Diagnostic and Configuration Port Protection
1139.01b1System.68	HITRUST 01.b User Registration
1173.01j1Organizational.6	HITRUST 01.j User Authentication for External Connections
1174.01j1Organizational.7	HITRUST 01.j User Authentication for External Connections
1175.01j1Organizational.8	HITRUST 01.j User Authentication for External Connections
11109.01q1Organizational.57	HITRUST 01.q User Identification and Authentication
11110.01q1Organizational.6	HITRUST 01.q User Identification and Authentication
11154.02i1Organizational.5	HITRUST 02.i Removal of Access Rights
11208.01q1Organizational.8	HITRUST 01.q User Identification and Authentication
11219.01b1Organizational.10	HITRUST 01.b User Registration
11220.01b1System.10	HITRUST 01.b User Registration
1111.01b2System.1	HITRUST 01.b User Registration
1112.01b2System.2	HITRUST 01.b User Registration
1125.01q2System.1	HITRUST 01.q User Identification and Authentication
1127.01q2System.3	HITRUST 01.q User Identification and Authentication
1128.01q2System.5	HITRUST 01.q User Identification and Authentication
1130.01v2System.1	HITRUST 01.v Information Access Restriction
1131.01v2System.2	HITRUST 01.v Information Access Restriction
1132.01v2System.3	HITRUST 01.v Information Access Restriction
1133.01v2System.4	HITRUST 01.v Information Access Restriction
1145.01c2System.1	HITRUST 01.c Privilege Management
1146.01c2System.23	HITRUST 01.c Privilege Management
1147.01c2System.456	HITRUST 01.c Privilege Management
1148.01c2System.78	HITRUST 01.c Privilege Management
1149.01c2System.9	HITRUST 01.c Privilege Management
1150.01c2System.10	HITRUST 01.c Privilege Management
11111.01q2System.4	HITRUST 01.q User Identification and Authentication
11112.01q2Organizational.67	HITRUST 01.q User Identification and Authentication
11200.01b2Organizational.3	HITRUST 01.b User Registration
11209.01q2Organizational.9	HITRUST 01.q User Identification and Authentication
11210.01q2Organizational.10	HITRUST 01.q User Identification and Authentication
11211.01q2Organizational.11	HITRUST 01.q User Identification and Authentication
1134.01v3System.1	HITRUST 01.v Information Access Restriction

12 Audit Logging & Monitoring

Audit Logs

FH Information Technology staff monitor the creation of audit logs. The data editing log for transactions in the FH Review Management System (the processing of PHI/PII Review data) include Date & Time of event, where (what form or screen) the event occurred, type of event, subject identity and outcome. Other logs monitored include service logs generated by the server (access, load measurements) and firewall logs. The log responsible for monitoring attempted logins (which fail) shall be reviewed. In the event a user attempts five unsuccessful logins, an email is generated and transmitted internally to the CIO, CSO and FH IT Staff. FOCUS shall maintain (store) all audit logs (with the exception of the Cisco ASA Firewall Log) for a minimum of 10 years. Cisco ASA Firewall logs, which are extremely large, shall be maintained (stored) for a period of at least 3 (three) months. Audit logs shall be protected from unauthorized access.

POLICY:
FOCUS shall provide notice that the employee's actions may be monitored, and that the employee consents to such monitoring. *1201.06e1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System has a comprehensive **audit log** of user actions; and that FOCUS IT has **administrative software** which allows end-user computer utilization monitoring; and a **screenshot** of the on-screen notification indicating that FOCUS Staff Member actions may be monitored. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the FOCUS Staff Member user interface screens within the FOCUS Review Management System to ensure compliance; and shall monitor the Audit Logs generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Training is to be provided regarding this policy to all FOCUS Staff Members and contract Peer Reviewers upon hire and annually thereafter that they read/understand/attest and comply with this policy; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Training logs to ensure that all applicable end users have received and attested to training; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that a secure audit record is created for all activities on the system (create, read, update, delete) involving covered information. *1202.09aa1System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures activities including reading, creation, modification and deletion of data within a comprehensive **audit log** of user actions; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the Audit Logs generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are tasked to ensure that the activity log is applicable to all users, maintained and functional at all times; and
— The activity log is to include creation/user ID/activity timestamps/function/before edit/after edit and deletion details; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that audit records include the unique user ID, unique data subject ID, function performed, and date/time the event was performed. *1203.09aa1System.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures the unique user ID, unique data subject ID, function performed, and date/time the event was performed; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the Audit Logs generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are tasked to ensure that the activity log is applicable to all users, maintained and functional at all times; and
— The activity log is to include user ID/unique data subject ID, function performed, and date/time the event was performed; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event. *1204.09aa1System.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Audit Logs**'. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures privileged user events including success/failure, time of occurrence, the account involved, process involved and additional information about the event; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Audit Logs generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are tasked to ensure that the activity log is applicable to all users, maintained and functional at all times; and
— The activity log is to include The activities of privileged users (administrators, operators, etc.) include the success/failure of the event, time the event occurred, the account involved, the processes involved, and additional information about the event; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that all applicable legal requirements related to monitoring authorized access and unauthorized access attempts are met. *1212.09ab1System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Access Logs**'. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures both successful and unsuccessful login attempts in the **Access Log**; and a **screenshot** of the access log is to be kept on file; and that the FOCUS CSO shall conduct legal compliance research for Federal, State and Contractural requirements monthly to ensure compliance regarding this topic. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the Access Logs generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Legal requirements are to be identified and documented within the FOCUS RMS Administration module/Compliance System, including the scope of Federal, State, Accreditors, Certifiers and client-company contracts regarding the collection and storage of monitoring data, including authorized access and unauthorized access attempts.
— The CSO schedules a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings for compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Documented, quarterly meeting minutes of audit logs, system settings and reporting; and
- Documented, monthly reviews of audit logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that separation of duties is used to limit the risk of unauthorized or unintentional modification of information and systems. *1229.09c1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas FOCUS IT Analysts have separation of duties so as to limit the risk of unauthorized or unintentional modification of information and systems; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the **Access Logs** generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to segregation of duties to determine if separation of duties or the monitoring of activities, audit trails, management supervision or a system of dual control when segregation is not possible is used to limit the risk of unauthorized or unintentional modification of information assets.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Separation of Duties (SoD) is integrated within the FOCUS RMS privilege sets, so as to limit the risk of unauthorized or unintentional modification of information and systems; and
— The implementation of SoD across FOCUS Employees and contracted Peer Reviewers is to be completed; and
— A documented quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings for compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Documented, quarterly meeting minutes of privilege sets ensuring separation of duties.

EVIDENCE:
- Company calendar; meeting minutes; privilege sets.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensures proper logging is enabled in order to audit administrator activities; and reviews system administrator and operator logs on a regular basis. *1270.09ad1System.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures administrator activities which are to be reviewed on a regular basis; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the **Audit Logs** generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are tasked to ensure that the activity log is applicable to all users, maintained and functional at all times; and
— The activity log is to include the activities of privileged users (administrators) on a regular basis; and
— The CSO is to schedule a quarterly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that an intrusion detection system managed outside of the control of system and network administrators is used to monitor system and network administration activities for compliance. *1271.09ad2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard whereas the FOCUS Review Management System automatically captures administrator activities which are to be reviewed monthly by the FOCUS Administrative Assistant, with any anomalies found to be reported to both the CEO and CSO; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the **Audit Logs** generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results, combined with any reported results from the FOCUS Administrative Assistant. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The RMS database server activity log, and the RMS audit log reveals all administrator level access and activity for compliance; and
— Document and schedule a monthly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; RMS database server logs; RMS audit logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall specify how often audit logs are reviewed, how the reviews are documented, and the specific roles and responsibilities of the personnel conducting the reviews, including the professional certifications or other qualifications required. *12101.09ab1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard, including frequency of audit log review, documentation of findings, the personnel assigned the responsibility of reviewing the logs and the required qualifications of the reviewer; and a **screenshot** of the audit log is to be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the **Audit Logs** generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results, combined with any reported results from the FOCUS Administrative Assistant. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The RMS database server activity log and the RMS audit log is to be reviewed monthly; and
— Document and schedule a monthly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and related quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; RMS database server logs; RMS audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall periodically test its monitoring and detection processes, remediate deficiencies, and improve its processes. *12102.09ab1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard, including periodic testing of monitoring and detection processes, remediate deficiencies and plan/document/execute processes. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the **Audit Logs** generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to audit and monitoring reviews to determine if the organization requires testing its monitoring and detection processes periodically , remediate deficiencies, and improve its processes.

PROCEDURES:
The FOCUS CSO ensure that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are to test the monitoring and detection processes, report deficiencies to the CSO, remediate the deficiencies, and ensure that monitoring and detection processes are optimized at all times.
— Document and schedule a monthly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitor:
- The company calendar to ensure compliance for policy reviews and related quarterly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; RMS database server logs; RMS audit logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Information collected from multiple sources shall be aggregated for review. *12103.09ab1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard, including aggregation of log data during the review and analysis process. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the **Audit Logs** generated by the FOCUS RMS Database Server, the FOCUS Review Management System audit logs; segments of the FOCUS security appliance (firewall) and to record **meeting minutes** of the report results. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the monitoring of system use and determine if the Information collected from multiple sources are aggregated and reviewed.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS RMS is to house the aggregated logs identified in the policy for inspection in the RMS Administration module/Logging System.
— Document and schedule a monthly meeting with FOCUS IT Analysts to confirm monitoring activity, reports and review system settings.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of quarterly meeting minutes of audit logs, system settings and reporting.

EVIDENCE:
- Company calendar; meeting minutes; RMS aggregated log inventory.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 12 AUDIT LOGGING AND MONITORING

1201.06e1Organizational.2	HITRUST 06.e Prevention of Misuse of Information Assets
1202.09aa1System.1	HITRUST 09.aa Audit Logging
1203.09aa1System.2	HITRUST 09.aa Audit Logging
1204.09aa1System.3	HITRUST 09.aa Audit Logging
1212.09ab1System.1	HITRUST 09.ab Monitoring System Use
1229.09c1Organizational.1	HITRUST 09.c Segregation of Duties
1270.09ad1System.12	HITRUST 09.ad Administrator and Operator Logs
1271.09ad2System.1	HITRUST 09.ad Administrator and Operator Logs
12101.09ab1Organizational.3	HITRUST 09.ab Monitoring System Use
12102.09ab1Organizational.4	HITRUST 09.ab Monitoring System Use
12103.09ab1Organizational.5	HITRUST 09.ab Monitoring System Use

13 Education, Training and Awareness

Training Policy related to Training Data

FOCUS provides training and re-training to Employees and contracted Peer Reviewers that is isolated from production data. Training sample data is of sample information with obviously generic person names (such as Test Test), etc. At no time will training be given on live systems containing PHI/PII production data.

Electronic Mail

As a productivity tool, FH encourages the use of electronic mail (email). However, users must be diligent in their efforts to prevent infection or transmission of infected emails. Specifically, email may deliver unsolicited messages that contain offensive content or malicious software (computer viruses, worms, etc.).
FH cannot guarantee email will be private. Email can, depending on the technology, be forwarded, intercepted, printed, and stored by others. People other than the intended recipient may possibly access email. Email may be stored in backups in systems that may be retrievable after traditional paper letters would have been discarded or destroyed. Staff should be aware email is analogous to sending a postcard such that the content is not protected.

All Users are prohibited from:

(1) Having their FH email accessed (e.g., POP'ed) from another email service, and
(2) Forwarding their FH email to another service; and
(3) Installing or accessing an employee FOCUS email account on any device not owned and provided by FH, including personal devices of any kind (computers, mobile phones, tablets); and
(4) Attempting to connect an external storage device (USB 'thumb' drive or external disk storage device).

In the course of their duties, FH Information Technology staff may need to look through users mailboxes in order to fix problems. But this is not to be done any more than is needed to correct the problem.

It is against FH policy (and numerous federal and state regulatory entities) for FH staff to email sensitive information. This includes any and all Patient Health Information (PHI), Personally Identifiable Information (PII), and clinical data. Further, FH staff members may not email company-confidential information.

Internet Use

Attempting to break into any computer system at anytime from any FH resource (e.g., computer or network) is strictly prohibited. Furthermore, releasing any worms or other malicious code out on the Internet, is prohibited. Attempting to subvert or avoid any FH electronic security system, or to bypass any network-based security mechanism is similarly prohibited.
Intentionally obtaining, sharing, storing, viewing, emailing, or downloading items of an obscene or graphic nature including but not limited to, pornographic, sexist, racist, or illegal materials and/or any information/graphics that violate any of the policies of FH is prohibited. Using FH resources to advertise or sell commercial products and/or services is strictly prohibited.

POLICY:
FOCUS shall ensure that employees and contractors receive documented initial (as part of their onboarding within sixty [60] days of hire), annual and ongoing training on their roles related to security and privacy. *1301.02e1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the policy and procedure supporting this standard; and the **FOCUS Onboarding Policy and Procedure**; and the FOCUS Training Agenda Policy and Procedure; and **screenshots** from the training functionality of the FOCUS Review Management System; and the **training attestation report** from the FOCUS Review Management System. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information security awareness, education, and training and determine whether awareness training commences with a formal induction process designed to introduce the organization's security and privacy policies, state and federal laws, and expectations before access to information or services is granted and no later than 60 days after the date the employee is hired. Further, ongoing training includes security and privacy requirements (e.g., objective, scope, roles and responsibilities, coordination, compliance, communicating threat information, legal responsibilities and business controls) as well as training in the correct use of information assets and facilities (e.g., including but not limited to log-on procedures, use of software packages, anti-malware for mobile devices, and information on the disciplinary process). Training discusses how the organization addresses each area (e.g., audit logging and monitoring); how events or incidents are identified (e.g., monitoring for inappropriate or failed user logins), and the actions the organization takes in response to events or incidents (e.g., notifying the workforce member or the members supervisor), as appropriate to the area of training.

PROCEDURES:
The FOCUS CSO ensures that:
— The FOCUS Training Agenda is updated to include curriculum that meets all topics required to ensure compliance with Federal, State, URAC, client-company contract, and HITRUST standards and requirements; and
— Ensuring that role-based training and measurements are defined; and
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are to receive documented initial (as part of their onboarding within sixty (60) days of hire), annual and ongoing training on their roles related to security and privacy; and
— No individual are to be permitted to access covered information until after initial training is complete; and
— All trainees must read/understand/attest and comply with all FOCUS policies and procedures.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes of training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that employees and contractors are informed in writing that violations of the security policies will result in sanctions or disciplinary action. *1306.06e1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes initial research regarding a suspected or actual violation; determination by FOCUS Administration and a documented notice in writing to the FOCUS Employee or contractor referring to the applicable violation level and disciplinary action, if applicable. Ongoing quality assurance includes thorough documentation of the suspected or actual violation within the FOCUS RMS Administration module/Staff records or FOCUS RMS Administration module/Peer Reviewer records or FOCUS RMS Administration module/contractor records; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are to receive documented initial (as part of their onboarding within sixty (60) days of hire), annual and ongoing training on their roles related to security and privacy; and
— No individual is to be permitted to access covered information until after initial training is complete; and
— Any suspected or actual violation must be documented and stored with the appropriate section of the RMS Administration module; and
— Upon final determination by FOCUS Administration, the Employee or contractor is informed, in writing, of the determination with violation description and disciplinary action.

Sanctions
It is the policy of FOCUS Health, Inc. that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. FOCUS Health will categorize violations and impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The sanctions will extend beyond protected health information that is in electronic form and include protected health information in written form.

FOCUS Health will take appropriate disciplinary action against employees, contractors, or any individuals who violate FOCUS Health's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

FOCUS Health has a rating system in place that is a reference for the appropriate personnel to utilize in addressing the disciplinary actions that should be taken according to the types of violations. The rating system is a three tier rating system and is available for viewing on page 7.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of reported suspected or actual violations to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; violation logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall define rules to describe user responsibilities and acceptable behavior for information system usage, including at a minimum, rules for email, internet, mobile devices, social media and facility usage. *1307.07c1Organizational.124* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FOCUS 2020 Code of Conduct.pdf**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure**; and the **FOCUS Code of Conduct**; and signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter of the preceding two policies and procedures. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to acceptable use of assets to determine if the organization establishes and makes readily available to all information system users, a set of rules that describe their responsibilities and expected behavior with regard to information and information system usage. Further, acceptable use addresses rules for electronic mail and Internet usages; and guidelines for the use of mobile devices, especially for the use outside the premises of the organization The organization includes in the rules of behavior, explicit restrictions on the use of social media and networking sites, posting information on commercial websites, and sharing information system account information.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training which includes the 'FOCUS 2020 Code of Conduct', whereby each recipient must read/understand/attest and comply with the Code of Conduct.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall prohibit users from installing unauthorized software, including data and software from external networks, and ensures users are made aware and trained on these requirements. *1308.09j1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Training**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** with signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training which includes this policy, whereby each recipient must read/understand/attest and comply with the prohibition of installing unauthorized software, including data and software from external networks, and ensures users are made aware and trained on these requirements.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that personnel using mobile computing devices are trained on the risks, the controls implemented, and their responsibilities, e.g., shoulder surfing, physical protections. *1309.01x1System.36* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Mobile Device Policy v 1.0.pdf**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure**; and the **FOCUS Code of Conduct**; and signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter of the preceding two policies and procedures. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training which includes this policy, whereby each recipient must read/understand/attest and comply with the responsibility of avoiding risks, the controls implemented, and their responsibilities .

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES & PROCEDURES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
FOCUS Mobile Device Policy

POLICY:
FOCUS shall ensure that personnel who telework are trained on the risks, the controls implemented, and their responsibilities. *1310.01y1Organizational.9* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Telecommuter Confidentiality v 12.0.pdf**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure**; and the **FOCUS Telecommuter Confidentiality Policy and Procedure**; and signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter of the preceding two policies and procedures. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to teleworking and determine whether training on security awareness, privacy and teleworker responsibilities are required prior to authorization.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are to be given training which includes this policy, whereby each recipient must read/understand/attest and comply with the responsibility of avoiding risks, the controls implemented, and their responsibilities.

MONITORING:
The FOCUS CSO monitor:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES & PROCEDURES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
FOCUS Telecommuter Confidentiality Policy

POLICY:
FOCUS shall provides training on BYOD usage, which includes providing an approved list of applications, application stores, and application extensions and plugins. *1326.02e1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. It is FOCUS policy that connecting or attempting to connect to the FOCUS network with a personal device via web browser or directly with VPN is strictly prohibited. FOCUS provides employees with company-owned devices which are secured through management software and other tools to prevent unauthorized access or loss of data. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure**; and the **FOCUS Telecommuter Confidentiality Policy and Procedure**; and signed **attestations** from all FOCUS Staff Members initially and annually thereafter of the preceding two policies and procedures. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS Policy prohibits employee end-users from attempting to access any application 'store'. Further, FOCUS employees are prevented from installing software on FOCUS owned computer systems by preventive control measures as part of baseline configuration requirements. Only the FOCUS IT Analyst, after FOCUS CSO testing and approval, may access software 'stores' to download and install software.

PROCEDURES:
It is FOCUS policy that connecting or attempting to connect to the FOCUS network with a personal device is strictly prohibited.
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Employees' privilege sets (e.g., FOCUS Staff, FOCUS Admin, etc.) will be configured to disallow web access to the RMS; and
— FOCUS Employees are given training which includes this policy, whereby each recipient must read/understand/attest and comply with the responsibility never attempting to connect a personally owned device of any type to the FOCUS network.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall provide incident response and contingency training to information system users consistent with assigned roles and responsibilities within ninety (90) days of assuming an incident response role or responsibility; when required by information system changes; and within every three hundred sixty-five (365) days thereafter. *1313.02e1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Training Agenda Policy and Procedure**; the **FOCUS Security Policy and Procedure** with signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter; and a series of **screenshots** of the FOCUS Review Management System PHI Reporting Functionality available on FOCUS Staff Member, Peer Reviewer and Client Portals. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to information security awareness, education, and training and determine whether the organization provides incident response and contingency training to information systems users consistent with assigned roles and responsibilities: (i) within 90 days of assuming an incident response role or responsibility; (ii) when required by information system changes; and, (iii) within every 365 days thereafter.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training within 90 days of hire (or contracting) and each year thereafter, to use a feature within the RMS that provides a venue to report security related incidents, including (but not limited to) PHI/PII being inadvertently transmitted over unsecure email, or a user of the system sharing their password over the phone or by writing it on paper by reading/understanding/attesting and complying with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs; screenshot of Incident Response Reporting System.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Employees, contractors and third party system users shall be made aware of the limits existing for their use of FOCUS's information and assets associated with information processing facilities and resources; and they are responsible for their use of any information resource and of any use carried out under their responsibility. *1324.07c1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Training**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that only FOCUS Staff Members, Peer Reviewers and Client-Companies shall have access to the FOCUS Review Management System; and that no time shall there be contractors, third party system users or any other entity given credentials to access the FOCUS Review Management System; and that FOCUS IT Staff Member training (with attestations) on procedures for data center access (requesting, revoking authorization for access via the CSO) are given initially and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this policy; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training prior to accessing PHI/PII within FOCUS systems with explicit instructions to never divulge or share credentials for access to FOCUS systems with anyone else; and
— FOCUS IT Analysts scheduled to receive privileges to access FOCUS data center resources are given training prior to data center access with explicit training not to ever divulge or share credentials for access to any FOCUS data center by reading/understanding/attesting and complying with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that personnel are appropriately trained on leading principles and practices for all types of information exchange (oral, paper and electronic). *1325.09s1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Training Agenda Policy and Procedure**; the **FOCUS Security Policy and Procedure** with signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training prior to accessing PHI/PII within FOCUS systems with explicit instructions to never verbally divulge OR print OR electronically share any protected information (patient records, company confidential records) by reading/understanding/attesting and complying with this policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The FOCUS security awareness and training program shall identify how workforce members are provided security awareness and training and the workforce members who will receive security awareness and training; and describes the types of security awareness and training that is reasonable and appropriate for its workforce members, how workforce members are provided security and awareness training when there is a change in FOCUS information systems, and how frequently security awareness and training is provided to all workforce members. *1336.02e1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Training Agenda Policy and Procedure**; the **FOCUS Security Policy and Procedure**; and the FOCUS Code of Conduct training with signed **attestations** from all FOCUS Staff Members and Peer Reviewers initially and annually thereafter; and **screenshots** of the FOCUS Review Management System training functionality. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, the Training Attestation Report generated by the FOCUS Review Management System; and to record **meeting minutes** of the report results to ensure compliance with all FOCUS Training Policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS Employees and contracted Peer Reviewers are given training prior to accessing PHI/PII within FOCUS systems with explicit instructions via teletraining (WebEx/Zoom) to view the Training Agenda, Security Policy and Code of Conduct documents to convey the FOCUS security awareness required before gaining access to PHI/PII and company confidential information (covered information) by reading/understanding/attesting and complying with this policy; and
— FOCUS Employees and contracted Peer Reviewers are to be given training annually during their employment or relationship with FOCUS; and
— Based on role and responsibilities in the organization, training will be provided on the complete FOCUS Security Policy and Procedure or the FOCUS Security Policy and Procedure (Simplified) version; and
— In the event there are changes in process, procedures or technology systems related to security, FOCUS is to provide interim training to Employees and contracted Peer Reviewers to ensure that any modifications in process or procedures are adhered to in an effort to maximized security and reduce risk.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR EDUCATION, TRAINING & AWARENESS

1301.02e1Organizational.12	HITRUST 02.e Information Security Awareness, Education, and Training
1306.06e1Organizational.5	HITRUST 06.e Prevention of Misuse of Information Assets
1307.07c1Organizational.124	HITRUST 07.c Acceptable Use of Assets
1308.09j1Organizational.5	HITRUST 09.j Controls Against malicious Code
1309.01x1System.36	HITRUST 01.x Mobile Computing and Communications
1310.01y1Organizational.9	HITRUST 01.y Teleworking
1326.02e1Organizational.4	HITRUST 02.e Information Security Awareness, Education, and Training
1313.02e1Organizational.3	HITRUST 02.e Information Security Awareness, Education, and Training
1324.07c1Organizational.3	HITRUST 07.c Acceptable Use of Assets
1325.09s1Organizational.3	HITRUST 09.s Information Exchange Policies and Procedures
1336.02e1Organizational.5	HITRUST 02.e Information Security Awareness, Education, and Training

14 Third Party Assurance

POLICY:
Access to FOCUSs information and systems by external parties shall not permitted until due diligence has been conducted, the appropriate controls have been implemented, and a contract/agreement reflecting the security requirements is signed acknowledging they understand and accept their obligations. *1401.05i1Organizational.1239* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that only FOCUS Staff Members, contracted Peer Reviewers and Client-Companies shall have access to the FOCUS Review Management System; and that no time shall there be contractors, third party system users or any other entity given credentials to access the FOCUS Review Management System; and that FOCUS IT Staff Member training (with attestations) on procedures for **data center access** (requesting, revoking authorization for access via the CSO) are given initially and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this policy; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to identification of risks related to external parties and determine if due diligence, including an evaluation of the information security risks posed by external parties, is carried out to identify any requirements for specific controls where access to sensitive information (e.g., covered information, cardholder data) by external parties is required prior to establishing a formal relationship with the service provider. Access by external parties to the organization's information is not be provided until the appropriate controls have been implemented and, where feasible, a contract has been signed defining the terms and conditions for the connection or access and the working arrangement. All security requirements resulting from work with external parties or internal controls are reflected by the agreement with the external party (see 5.i and 5.j). It is ensured that the external party is aware of their obligations, and accepts the responsibilities and liabilities involved in accessing, processing, communicating, or managing the organization's information and information assets.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are to be given training by reading/understanding/attesting that only FOCUS Staff Members, contracted Peer Reviewers and Client-Companies are to have access to the FOCUS Review Management System; and that no time is there to be contractors, third party system users or any other entity given credentials to access the FOCUS Review Management System; and
— FOCUS IT Analysts are to be given training by reading/understanding/attesting that only FOCUS CSO and IT Analysts are to have access to FOCUS data center(s).

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Remote access connections between FOCUS and external parties shall be encrypted. *1402.05i1Organizational.45* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that all data traffic must be encrypted either by Virtual Private Network (VPN) or Secure Socket Layer (SSL) certificates; and **screenshots** of the VPN configuration shall be on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this policy and VPN configuration screenshots; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to identification of risks related to external parties and determine if all remote access connections between the organization and all external parties are secured via encrypted channels (e.g., VPN). Any covered information shared with an external party is encrypted prior to transmission.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are to be given training by reading/understanding/attesting that remote access connections between FOCUS and external parties are encrypted; and
— FOCUS IT Analysts are to make screenshots and report these to the CSO on a quarterly basis showing evidence that websites are encrypted via SSL and that FOCUS employees utilize VPN to access the FOCUS network.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs; screenshots.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that access granted to external parties is limited to the minimum necessary and granted only for the duration required. *1403.05i1Organizational.67* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This policy stipulates that only FOCUS Staff Members, contracted Peer Reviewers and Client-Companies shall have access to the FOCUS Review Management System. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that the session for all users must be automatically disconnected from the FOCUS Review Management System, based on their role, to provide minimum necessary access that is granted only for the duration required to perform the users' function; and **screenshots** of the resulting disconnection; and in the event a user does not access the FOCUS Review Management System for a period of 30 days, their access is suspended and must be re-authenticated by calling the FOCUS Technical Support (FOCUS IT Analyst) team. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this policy and session discontinuation screenshots; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to identification of risks related to external parties and determine if external parties are granted minimum necessary access to the organization's information assets to minimize risks to security. All access granted to external parties is limited in duration and revoked when no longer needed.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS IT Analysts are to be given training by reading/understanding/attesting that only FOCUS Staff Members, contracted Peer Reviewers and Client-Companies are to have access to the FOCUS Review Management System; and
— FOCUS IT Analysts ensure that the session for all users must be automatically disconnected from the FOCUS Review Management System, based on their role, to provide minimum necessary access that is granted only for the duration required to perform the users' function; and
— FOCUS IT Analysts must provide screenshots as evidence of automated system disconnections.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs; screenshots.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
A standard agreement with third parties shall be defined and includes the required security controls in accordance with FOCUS's security policies. *1406.05k1Organizational.110* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that all users must sign in attestation to the FOCUS Confidentiality Agreement (**Confidentiality and Non-Disclosure Agreement.pdf**) initially and annually thereafter; and that FOCUS must have a fully executed Business Associate Agreement (BAA) on file for each Data Center contracted; and that FOCUS must have the SOC-2 and HIPAA report on file from each Data Center. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this policy attestations to the FOCUS Security Policy and Procedure attestations, the FOCUS Confidentiality Agreement attestations; the executed BAA, SOC-2 and HIPAA documentation from Data Center Contractors; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS contracted Peer Reviewers must execute (sign) the 'Confidentiality and Non-Disclosure Agreement' before being granted access to PHI/PII; and
— Contracted vendors (i.e., data centers, VoIP telephony vendors, penetration testing vendors) must have a fully executed Business Associate Agreement (BAA) on file and 'Confidentiality and Non-Disclosure Agreement' executed before services may commence.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs; Business Associate Agreements, Confidentiality and Non-Disclosure Agreements.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that Service Level Agreements (SLAs) or contracts with an agreed service arrangement address liability, service definitions, security controls, and other aspects of services management. *1408.09e1System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS must have a fully executed Service Level Agreement (SLA) and Business Associate Agreement (BAA) on file to address liability, service definitions, security controls and other aspects of services management; and a fully executed FOCUS Confidentiality Agreement. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, the FOCUS policy, the executed BAA, the executed SLA and Confidentiality Agreement; and to record **meeting minutes** to ensure compliance with this policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Vendors must have a fully executed Service Level Agreement (SLA) and Business Associate Agreement (BAA) on file to address liability, service definitions, security controls and other aspects of services management; and a fully executed Confidentiality and Non-Disclosure Agreement (NDA).

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of monthly meeting minutes and training logs to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; training logs; Business Associate Agreements, Confidentiality and Non-Disclosure Agreements, Service Level Agreements.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the results of monitoring activities of third-party services are compared against the Service Level Agreements or contracts at least annually. *1411.09f1System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Agreements**'. Evidence of meeting this standard includes monthly meetings with the FOCUS CSO and FOCUS IT Analyst staff members to document assessments in meeting minutes of each third party service provider's Service Level Agreements and the results of those assessments; and that the FOCUS Review Management System **Supplier Inventory Tracking** function shall include contact information, Agreements and supporting documents for each vendor; and the FOCUS CSO shall review, on a quarterly basis, the executed SLA Agreements with third-party service providers and to record **meeting minutes** to report findings and any identified lapses in service or security protocols. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Third party servicer service level agreements or contracts are to be reviewed at least annually to monitor activities and ensure compliance.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of third party servicer service level agreements or contracts.

EVIDENCE:
- Company calendar; meeting minutes; training logs; Service Level Agreements.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Where software development is outsourced, formal contracts shall be written and fully executed to address the ownership and security of the code and application. *1416.10l1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that software development outsourcing is not to be initiated without the express authorization by the CEO and CSO; however, in the event software development is outsourced, the CSO shall ensure that appropriate language is incorporated into Agreements to address ownership and security of the code and application. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy and to record **meeting minutes** to ensure compliance and current status of software development outsourcing. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the outsourcing of software development and determine if outsourced software development contracts address licensing arrangements, code ownership, intellectual property rights, certification and rights of access for the audit of the quality and accuracy of work, escrow arrangements, quality and security functionality requirements for the developed code, and security testing and evaluation prior to installation.

NOTE: As of the time of this policy effective date, FOCUS does not outsource software development.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— In the event software development outsourcing may be required, this policy is to be modified to ensure that formal contracts are in place to address the ownership and security of the code and application.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and annual meetings.

EVIDENCE:
- Company calendar; meeting minutes.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that customers are aware of their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing FOCUS's information and information assets. *1419.05j1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS Agreements with client-companies must stipulate client-company obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing FOCUS's information and information assets; and a **redacted contract** shall be on file. Further, the **Terms of Service** policy which shall be made available on the FOCUS login page for client-company end users to have access to prior to logging into the FOCUS system, as well as availability of this policy on the main menu of the FOCUS RMS client portals, to explain obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing FOCUS's information and information assets. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy to ensure compliance with current and potential clients and to record **meeting minutes** to document the status of all client-company Agreements with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to addressing security when dealing with customers to determine if the following security terms are addressed prior to giving customers access to any of the organization's assets: (i) description of the product or service to be provided; (ii) the right to monitor, and revoke, any activity related to the organization's assets; and, (iii) the respective liabilities of the organization and the customer. It is ensured that the customer is aware of their obligations, and accepts the responsibilities and liabilities prior to accessing, processing, communicating, or managing the organization's information and information assets.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy stipulates that FOCUS Agreements with client-companies must stipulate their obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing FOCUS's information and information assets; and a **redacted contract** must be on file; and
— The **Terms of Use** policy which is to be made available on the FOCUS login page for client-company end users to have access to prior to logging into the FOCUS system, as well as availability of this policy on the main menu of the FOCUS RMS client portals, to explain obligations and rights, and accept the responsibilities and liabilities involved in accessing, processing, communicating, or managing FOCUS's information and information assets.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Monitoring of third party servicer service level agreements or contracts.

EVIDENCE:
- Company calendar; meeting minutes; Terms of Use policy.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall permit an individual to request restriction of the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or health care operations, and is not for purposes of carrying out treatment, and responds to any requests from an individual on the disclosure of the individual's covered information. *1420.05jHIPAAOrganizational.34* This requirement is stipulated in the **Consumer Communications Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **Consumer Communications Policy and Procedure** which specifies that (1) At no time shall a FOCUS employee, contracted Peer Reviewer nor their assistant divulge or confirm any information relating any client-company members (patients); and (2) The FOCUS employee, contracted Peer Reviewer or assistant must politely explain that no information is available and that they must contact their insurance carrier's Care Manager; and (3) If the caller asks to speak to a manager, the response is the same -- that their next step is to contact their insurance carrier Care Manager; and (4) If they do not know who their Care Manager is, indicate that no information is available. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy; and to record **meeting minutes** to document any reported incidents of incoming client-company member communications. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to addressing security when dealing with customers to determine if the organization permits an individual to request to restrict the disclosure of the individual's covered information to a business associate for purposes of carrying out payment or healthcare operations, and is not for purposes of carrying out treatment. The organization responds to any requests from an individual on the disclosure of the individual's covered information, providing the individual with records (see 06.c) of disclosures of covered information that are made by the organization and either:
(i) records (see 06.c) of disclosures of covered information made by a business associate acting on behalf of the organization; or, (ii) a list of all business associates acting on behalf of the covered entity, including contact information for such associates (such as mailing address, phone, and email address).

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— At no time is a FOCUS employee, contracted Peer Reviewer nor their assistant divulge or confirm any information relating any client-company members (patients); and
— The FOCUS employee, contracted Peer Reviewer or assistant must politely explain that no information is available and that they must contact their insurance carrier's Care Manager; and
— If the caller asks to speak to a manager, the response is the same -- that their next step is to contact their insurance carrier Care Manager; and (4) If they do not know who their Care Manager is, indicate that no information is available.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings.

EVIDENCE:
- Company calendar; meeting minutes; Consumer Communications Policy.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES & PROCEDURES:
Location of policy: RMS -> ADMIN -> ORGANIZATION -> P&Ps
FOCUS Consumer Communications Policy

POLICY:
FOCUS shall identify and mandates information security controls to specifically address supplier access to FOCUS's information and information assets. *1428.05k1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS identifies and mandates information security controls to specifically address supplier access to FOCUS information and information assets; and that FOCUS maintains a fully executed Business Associate Agreements (BAA) for each Data Center; and that FOCUS maintains a fully executed FOCUS Confidentiality Agreement for each Data Center; and that each Data Center provides FOCUS a current SOC-2 report which must be kept on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy and BAA agreements and SOC-2 reports and Confidentiality Agreement; and to record **meeting minutes** to document the findings and status of these Agreements with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS identifies and mandates information security controls to specifically address supplier access to FOCUS' information and information assets; and
— FOCUS maintains a fully executed Business Associate Agreements (BAA) for each Data Center; and
— FOCUS maintains a fully executed FOCUS Confidentiality Agreement for each Data Center; and
— Each Data Center provides FOCUS a current SOC-2 report which must be kept on file.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- All BAA, NDA and SOC-2 reports are to be monitored and reviewed quarterly.

EVIDENCE:
- Company calendar; meeting minutes; BAA, NDA and SOC-2 reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain written agreements (contracts) that include: (i) an acknowledgement that the third party (e.g., a service provider) is responsible for the security of the data and requirements to address the associated information security risks and (ii) requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain. *1429.05k1Organizational.34* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Supplier Agreements**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS prohibits the use of 'cloud computing' data storage, and that FOCUS only engages in 'server co-location' services with a data center vendor; and that FOCUS has written, fully executed **Agreements** with each data center that includes language that each data center supplier is responsible for the security of the data and requirements to address the associated information security risks. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy and Agreements with each Data Center; and to record **meeting minutes** to document the findings and status of these Agreements with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to addressing security in third-party agreements and determine if agreements include requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain. The organization maintains written agreements (contracts) that includes an acknowledgement that the third-party (e.g., service provider) is responsible for the security of the data the third-party possesses or otherwise stores, processes or transmits on behalf of the organization, or to the extent that they could impact the security of the organizations information environment.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are to be reviewed/modified/ratified no less than annually; and
— FOCUS maintains written agreements (contracts) that include:
  - An acknowledgement that the third party (e.g., a service provider) is responsible for the security of the data and requirements to address the associated information security risks; and
  - Requirements to address the information security risks associated with information and communications technology services (e.g., cloud computing services) and product supply chain.

— FOCUS maintains a fully executed Business Associate Agreements (BAA) for each service provider.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and monthly meetings; and
- Business Associate Agreements are to be monitored and reviewed quarterly.

EVIDENCE:
- Company calendar; meeting minutes; Business Associate Agreements.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The agreement shall ensure that there is no misunderstanding between FOCUS and the third party and satisfies FOCUS as to the indemnity of the third party. *1430.05k1Organizational.56* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS **Agreements** with third parties (Data Centers) are clearly written to ensure FOCUS as to the indemnity of the third party. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy and Agreements with each Data Center; and to record **meeting minutes** to document the findings and status of these Agreements with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Agreements are clearly written, and satisfies FOCUS as to the indemnity of the third party; and
— As needed, Agreements are to be vetted by FOCUS legal counsel.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Business Associate Agreements are to be monitored and reviewed quarterly.

EVIDENCE:
- Company calendar; meeting minutes; Business Associate Agreements.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall establish personnel security requirements, including security roles and responsibilities, for third-party providers that are coordinated and aligned with internal security roles and responsibilities. *1431.05k1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS **Agreements** with third parties (e.g., Data Centers) clearly indicate security roles and responsibilities of appointed FOCUS Staff Members by title, to ensure coordination and alignment with third-party providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy, appointed FOCUS staff members by title, and Agreements with each Data Center; and to record **meeting minutes** to document the findings and status of these assignments and Agreements with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance, including appointed FOCUS staff members by title, and Agreements with each Data Center; and
— FOCUS IT Analysts are to be provided training to read/understand/attest and comply with this policy, including attesting to the FOCUS Security Policy and;
— FOCUS third-party provider Agreements (e.g., data centers) is to include security commitments as provided by the data center certifications which the CSO is to have on file within the RMS for review; and
— FOCUS contracted Peer Reviewers are to be provided training to read/understand/attest and comply with this policy, including attesting to the FOCUS Security Policy.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- FOCUS training attestations to ensure compliance; and
- FOCUS Agreements with data centers and ensure that data center certifications on file are up-to-date and stored within the RMS.

EVIDENCE:
- Company calendar; meeting minutes; training attestations; data center agreements; data center certifications.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure a screening process is carried out for contractors and third party users; and, where contractors are provided through an organization, (i) the contract with FOCUS clearly specifies FOCUS's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern and, in the same way, (ii) the agreement with the third party clearly specifies all responsibilities and notification procedures for screening.
1432.05k1Organizational.89 This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Supplier Agreements**'. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS **Agreements** with third parties (Data Centers) clearly indicate that FOCUS shall conduct screening processes as well as the notification process, including procedures the vendor needs to follow in the event results give cause for doubt or concern; and the Agreement with the third party clearly specifies all responsibilities and notification procedures for screening. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy, the inventory of third party users and contractors, and monitor the status and frequency of screening for each; and to record **meeting minutes** to document the findings and status of these third parties, their respective Agreements and screenings with FOCUS. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to addressing security in third-party agreements and determine if the organization ensures a screening process is carried out for contractors and third-party users. Where contractors are provided through an organization: (i) the contract with the organization clearly specifies the organizations responsibilities for screening and the notification procedures they need to follow if screening has not been completed, or if the results give cause for doubt or concern, and (ii) in the same way, the agreement with the third-party clearly specifies all responsibilities and notification procedures for screening.

NOTE: It is FOCUS policy that no Data Center employees or data center contractors are to be given access to any FOCUS data.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— FOCUS is to comply with all laws regarding authorizations for background checks and other security elements prior to research; and
— FOCUS ensures a screening process is carried out prior to contractor access to any covered data; and
— For contractors and third party users which includes:
  • Data Centers: backgrounds checks, OIG and GSA reports, and active data center certifications; and
  • Clinicians: OIG and GSA reports, and NPDB reports; and
— Where contractors are provided through an organization:
  • The contract with FOCUS clearly specifies FOCUS's responsibilities for screening and the notification procedures they need to follow if screening has not been completed or if the results give cause for doubt or concern; and
  • The agreement with the third party clearly specifies all responsibilities and notification procedures for screening.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Quarterly documented review of the inventory of third party users and confirmation of background authorizations on file in meeting minutes; and
- Quarterly documented review of contractor Agreements to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; background check authorizations; background check reports; OIG/GSA reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the identification of risks related to external party access takes into account a minimal set of specifically defined issues. *1418.05i1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that when conducting the **FOCUS Risk Assessments v4.0**, a minimal set of specifically defined issues related to external party access must be included; and the FOCUS Risk Assessment must be conducted annually and maintained on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy, and ensure that the FOCUS Risk Assessment contains elements specifically addressing external party access; and to record **meeting minutes** to document the review and status of the FOCUS Risk Assessment and ensure that external party access is secure. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to external party access and validate the identification of risks related to external party access take into account the following issues:
i. the information asset(s) an external party is required to access;
ii. the type of access the external party will have to the information and information asset(s), such as:
   1. physical access (e.g. to offices, computer rooms, filing cabinets),
   2. logical access (e.g. to an organization's databases, information systems),
   3. network connectivity between the organization's and the external party's network(s) (e.g. permanent connection, remote access), and
   4. whether the access is taking place on-site or off-site;
iii. the value and sensitivity of the information involved, and its criticality for business operations;
iv. the controls necessary to protect information that is not intended to be accessible by external parties;
v. the external party personnel involved in handling the organization's information;
vi. how the organization or personnel authorized to have access can be identified, the authorization verified, and how often this needs to be reconfirmed;
vii. the different means and controls employed by the external party when storing, processing, communicating, sharing and exchanging information;
viii. the impact of access not being available to the external party when required, and the external party entering or receiving inaccurate or misleading information;
ix. practices and procedures to deal with information security incidents and potential damages, and the terms and conditions for the continuation of external party access in the case of an information security incident;
x. legal and regulatory requirements and other contractual obligations relevant to the external party are taken into account; and
xi. how the interests of any other stakeholders may be affected by the arrangements.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— A risk assessment, which is to include specific issues regarding potential risks posed by contractor relationships (data centers contracted Peer Reviewers).

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Quarterly documented review of the risk assessment elements, including external party access in meeting minutes; and
- Quarterly documented review of contractor Agreements to ensure compliance.

EVIDENCE:
- Company calendar; meeting minutes; Risk Assessment policy.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
FOCUS Risk Assessment

POLICY:
FOCUS shall develop, disseminate and annually review/update a list of current service providers, which includes a description of services provided. *1409.09e2System.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure indicates that the FOCUS Review Management System must provide a **supplier inventory function** which contains contact information, supplier services, Agreements and supporting documents and generates reports of past and present suppliers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, this FOCUS policy, and ensure that the FOCUS Review Management System supplier inventory function is up-to-date with supplier information and documentation; and to record **meeting minutes** to document the review and status and completeness of the FOCUS supplier inventory function. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— The FOCUS RMS Administrative module/Vendor system is to contain a list of all vendor names, website, representatives and their contact information, description of vendor services, binary files for agreements and metadata files.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Quarterly documented review of vendor inventory and all associated data.

EVIDENCE:
- Company calendar; meeting minutes; vendor list.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall address information security and other business considerations when acquiring systems or services; including maintaining security during transitions and continuity following a failure or disaster. *1410.09e2System.23* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure indicates that all security elements must be considered upon acquisition of systems or services, including transitions or failure or disasters. Additional specifics may be found in the **FOCUS Change Management Policy** regarding FOCUS IT Services or service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, and ensure that all system or service acquisition processes include security reviews; and to record **meeting minutes** to document acquisitions of systems or services, transitions or failures or disasters with notations regarding the criticality of security continuity. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to service delivery to determine, in the case of outsourcing arrangements, the organization plans the necessary transitions (of information, information processing systems, and anything else that needs to be moved), and ensures that security is maintained throughout the transition period. The organization ensures that the third-party maintains sufficient service capabilities together with workable plans designed to ensure that agreed service continuity levels are maintained following major service failures or disaster.

NOTE: It is FOCUS policy that at no time shall security policies and procedures be circumvented, regardless of business urgency.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— FOCUS IT Analysts are to be trained to review all applicable security policies within this document to ensure that information security and other business considerations are applied:
  • When FOCUS has acquired systems or services; and
  • When transitioning systems or services; and
  • Following a system or services failure or disaster.

MONITORING:
The FOCUS CSO monitors:
• The company calendar to ensure compliance for policy reviews and quarterly reviews; and
• Quarterly documented review of training logs, that hardware/services acquisitions or failures/disasters did not, at any point, reduce security for covered information.

EVIDENCE:
• Company calendar; meeting minutes; effective policy.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that regular progress meetings are conducted as required by the SLA to review reports, audit trails, security events, operational issues, failures and disruptions, and identified problems/issues are investigated and resolved accordingly. *1412.09f2System.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes quarterly reviews of SLAs by the FOCUS CSO to document assessments in meeting minutes of each client-company Service Level Agreement, and vendor (third party) service provider's Service Level Agreements and the results of those assessments; and that the FOCUS Review Management System **Supplier Inventory Tracking** function shall include contact information, Agreements and supporting documents for each vendor, and identify lapses in service or security protocols to be resolved. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the monitoring and review of third-party services to determine if service reports produced by the third-parties be reviewed and regular progress meetings are arranged as required by the agreements. Third-party audit trails and records of security events, operational problems, failures, tracing of faults and disruptions related to service delivery will be reviewed. Information about information security incidents are provided to the incident response team. This information is reviewed by the third-party that experienced the incident and the organization which the third-party provides services to as required by the agreements and any supporting guidelines and procedures. Any identified problems are resolved and reviewed by the organization as noted above.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
—.Service Level Agreements with vendors are to be reviewed, including reports, audit trails, security events, operational issues, failures and disruptions, and identified problems/issues are investigated and resolved accordingly; and
— Service Level Agreements with client-companies are to be reviewed, including reports, audit trails, security events, operational issues, failures and disruptions, and identified problems/issues are investigated and resolved accordingly.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Quarterly documented review of all SLAs, with documented evidence of review outcomes and mitigation (if found) to be entered into the RMS Administrative module.

EVIDENCE:
- Company calendar; meeting minutes; effective policy; SLA review reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that network services are periodically audited to ensure that providers have implemented the required security features and meet the requirements agreed with management, including new and existing regulations. *1413.09f2System.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes semi-annual audits by the FOCUS CSO to document audits in meeting minutes of each third party service provider's security features and meet the requirements agreed to with FOCUS, including new and existing regulations; and the results of those assessments; and the FOCUS CSO shall meet with each network services vendor, on the alternating semi-annual basis, the executed SLA Agreements with third-party service providers and to record **meeting minutes** to report findings and any identified lapses and/or corrections by network providers. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Network Service Provider Agreements, documented security features and regulatory requirements are audited semi-annually with results documented within the RMS Administration module; and
— Network Service Provider meetings are to be held on the alternating semi-annual basis to document discussions held to review required security features agreed with management, including new and existing regulations.

MONITORING:
The FOCUS CSO monitors:
- The company calendar to ensure compliance for policy reviews and quarterly reviews; and
- Semi-annual review of agreements; and
- Semi-annual meeting with Network Services representatives.

EVIDENCE:
- Company calendar; semi-annual meeting minutes; effective policy; semi-annual audits.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall employ a service management relationship and process between itself and a third party to monitor (i) security control compliance by external service providers on an ongoing basis; and (ii) network service features and service levels to detect abnormalities and violations. *1442.09f2System.456* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes FOCUS policy which stipulates that FOCUS shall contract a third party to evaluate FOCUS' security control compliance, and to evaluate network service features and service levels to detect abnormalities and violations; and that the FOCUS CSO shall conduct **meeting minute** (documented) semi-annually to review findings and ensure that any cited modifications are made to ensure compliance and correct abnormalities or violations. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Network Service Provider tele-meetings are held semi-annually between the CSO and vendor, to maintain a service management relationship and process to monitor:
  • Security control compliance by external service providers on an ongoing basis; and
  • Network service features and service levels to detect abnormalities and violations.

MONITORING:
The FOCUS CSO monitors:
• Semi-annual meeting with vendor of Network Services representatives.

EVIDENCE:
• Company calendar; semi-annual meeting minutes; effective policy.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall restrict the location of facilities that process, transmit or store covered information (e.g., to those located in the United States), as needed, based on its legal, regulatory, contractual and other security and privacy-related obligations. *1464.09e2Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS CSO shall conduct **meeting minute** (documented) monthly compliance research to ensure that FOCUS is compliant with federal, state and contractural requirements; and the FOCUS CSO shall review, on a quarterly basis, the compliance findings, client-company Agreements and to record **meeting minutes** to report findings and confirm that all communications are limited to US stakeholders. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that processing, transmitting or storing information outside of the US is strictly prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Client-company Terms of Use policy; Peer Reviewer and FOCUS Employee training attestations are to provide evidence that it is FOCUS policy that processing, transmitting or storing information outside of the US is strictly prohibited.

MONITORING:
The FOCUS CSO monitors:
- Semi-annual meeting with vendor of Network Services representatives; company calendar entries for quarterly review of policy.

EVIDENCE:
- Company calendar; semi-annual meeting minutes; effective policy; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The service provider shall protect FOCUS data with reasonable controls (e.g., policies and procedures) designed to detect, prevent, and mitigate risk. *1438.09e2System.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the **FOCUS Security Policy and Procedure** which specifies that FOCUS third parties (Data Centers) have provided FOCUS with certification and accreditation evidence such as SOC-2 Reports, HiTrust certification, SSAE, FISMA, FERPA, PCI or others. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a semi-annual basis, this FOCUS policy, the inventory of third party certifications, and monitor the status and expiration of these certifications; and to record **meeting minutes** to document the findings and status of these third party certifications. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Data centers are to provide FOCUS with certification and accreditation evidence such as SOC-2 Reports, HiTrust certification, SSAE, FISMA, FERPA, PCI or others.

MONITORING:
The FOCUS CSO monitors:
- Semi-annual review of service provider controls (policies & procedures) to ensure compliance.

EVIDENCE:
- Company calendar; semi-annual meeting minutes; effective policy.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 14 THIRD PARTY ASSURANCE

1401.05i1Organizational.1239	HITRUST 05.i Identification of Risks Related to External Parties
1402.05i1Organizational.45	HITRUST 05.i Identification of Risks Related to External Parties
1403.05i1Organizational.67	HITRUST 05.i Identification of Risks Related to External Parties
1406.05k1Organizational.110	HITRUST 05.k Addressing Security in Third Party Agreements
1408.09e1System.1	HITRUST 09.e Service Delivery
1411.09f1System.1	HITRUST 09.f Monitoring and Review of Third Party Services
1416.10l1Organizational.1	HITRUST 10.l Outsourced Software Development
1419.05j1Organizational.12	HITRUST 05.j Addressing Security When Dealing with Customers
1420.05jHIPAAOrganizational.34	HITRUST 05.j Addressing Security When Dealing with Customers
1428.05k1Organizational.2	HITRUST 05.k Addressing Security in Third Party Agreements
1429.05k1Organizational.34	HITRUST 05.k Addressing Security in Third Party Agreements
1430.05k1Organizational.56	HITRUST 05.k Addressing Security in Third Party Agreements
1431.05k1Organizational.7	HITRUST 05.k Addressing Security in Third Party Agreements
1432.05k1Organizational.89	HITRUST 05.k Addressing Security in Third Party Agreements
1418.05i1Organizational.8	HITRUST 05.i Identification of Risks Related to External Parties
1409.09e2System.1	HITRUST 09.e Service Delivery
1410.09e2System.23	HITRUST 09.e Service Delivery
1412.09f2System.12	HITRUST 09.f Monitoring and Review of Third Party Services
1413.09f2System.3	HITRUST 09.f Monitoring and Review of Third Party Services
1442.09f2System.456	HITRUST 09.f Monitoring and Review of Third Party Services
1464.09e2Organizational.5	HITRUST 09.e Service Delivery
1438.09e2System.4	HITRUST 09.e Service Delivery

15 Incident Management

Reporting an Incident

It is the responsibility of any FH Staff Member or Peer Reviewer aware of a security incident to report it immediately to the FH Chief Security Officer or the FH Information Technology help desk (866) 561-9542. There is also an option to report a security incident or threat within the FH RMS system by clicking on 'My FOCUS Life' on the main menu, and selecting 'Security Incident'. The FH Chief Security Officer will then investigate the incident, notify affected parties (if needed), and recommend corrective actions.

FH Client Company end-users are also able to call the above help desk or, within the RMS web portal, click on 'Report a Security Incident' on their main menu as well. Futher, the FOCUS public website provides a button for anyone to anaonamously file a complaint or concern.

Security Incident Response Procedures

This section provides analysis and procedures for preventing information security incidents. Some examples of possible incident categories to prevent include:

- Compromise of system integrity (Hacker/Cracker)
- Denial of service of system resources
- Malicious use of system resources
- Virus, Worm, Malware, or Trojan infection

The main tasks involved in preventing security incidents are preventing unauthorized access or use of the system or the data contained therein.

The term incident in this document is defined as any irregular or adverse event that occurs on any part of the FOCUS network. Some examples of possible incident categories include: compromise of system integrity; denial of system resources; illegal access to a system (either a penetration or an intrusion); malicious use of system resources, or any kind of damage to a system. Some possible scenarios for security incidents are:

- The discovery of a strange process running and accumulating a lot of CPU time.
- The discovery that an intruder logged into the system.
- The discovery of a virus that has infected the system.
- The discovery that someone from a remote site is trying to penetrate a system.

General Guidelines

In many cases, the actions outlined in this guideline will not be performed by a single person on a single system. Many people may be involved during the course of an active security incident that affects several of the FOCUS systems at one time (i.e., a worm attack). The FOCUS CSO should always be involved in the investigation of any information security incident.

The incident response team is made up of the FOCUS CSO, as required. The FOCUS CSO will be responsible for assigning people to work on specific tasks of the incident handling process and will coordinate the overall incident response process. All people involved in the incident response and cleanup are responsible for providing any needed information to members of the incident response team. Any directives given by a member of the incident response team will supersede this document.

Important Considerations

Urgency: A computer security incident can occur at any time of the day or night, and should be addressed with as much expediency as possible.

Discretion: A security breach may involve many different people. As a result, disclosure to parties outside of the incident response team or members of senior management of FOCUS may be seen as breach of confidence and possible complicity. The media especially is an important consideration. If someone from the media obtains knowledge about a security incident, they will attempt to gather further knowledge for probable publication. Providing information to the wrong people could have undesirable side effects. Any release of information will be at the discretion of the CEO or designee. Requests for information regarding a security incident must be forwarded to the CEO or designee.

Keep a Log book: Logging of information is critical in situations that may eventually involve a criminal trial. The implications from each security incident are not always known at the beginning of, or even during, the course of an incident. Therefore, a written log should be kept for all security incidents that are under investigation. The information should be logged in a location that cannot be altered by others. Manually written logs are preferable since online logs can be altered or deleted. The types of information that should be logged are:

- Dates and times of incident-related phone calls.
- Dates and times when incident-related events were discovered or occurred.
- Amount of time spent working on incident-related tasks.
- People you have contacted or have contacted you.
- Names of systems, programs, or networks that have been affected.

Follow-Up Analysis: After an incident has been fully handled and all systems are restored to a normal mode of operation, a follow-up postmortem analysis should be performed. The follow-up stage is one of the most important stages for handling a security incident. All involved parties (or a representative from each group) should meet and discuss actions that were taken and the lessons learned. All existing procedures should be evaluated and modified, if necessary. All online copies of infected files, worm code, etc., should be removed from the system(s).

INCIDENT SPECIFIC PROCEDURES

Physical Security Compromise

Only authorized people are allowed into restricted areas with access to information assets per the guidelines set forth policy and procedure. If an individual is detected attempting to access secured information assets, first attempt to confirm if the person is authorized access. If unauthorized access can be sufficiently confirmed, the FOCUS CSO, his or her designee, should be notified. The FOCUS CSO, his or her designee, will take appropriate action. **Do not attempt to confront the intruder.**

System Integrity Compromise (Hacker/Cracker)

Responding to hacker/cracker incidents is somewhat different than responding to a worm or virus incident. Some hackers are very sophisticated and will go to great depths to avoid detection. Others are naïve, young, and looking for a little excitement. A hacker can also be someone on the inside engaging in illicit system activity (i.e., password cracking). Any hacker/cracker incident needs to be addressed as a real threat to FOCUS systems and data. Hacker incidents can be divided into three types of responses: Attempt, Active or Inactive.

Attempted Intrusions

Intrusion attempts include: repeated login attempts, telnet commands, port scans, and repeated dial-back attempts. These activities can be viewed as hostile and must be mitigated. Under the direction of the FOCUS CIO, the following action will be taken:

- **Confirm** the attempted intrusions by trying to determine intent and or legitimacy. It is possible that what appears to be an attempted intrusion is really an anomaly in Internet traffic patterns or ISP activity.
- **Identify source** of the attack(s) by looking at system log files and active network connections. Make copies of all audit trail information such as system logs files and store them in a safe place. Capture process status information in a file and then store the file in a safe place. Log all actions.
- **Isolate** the attacker to prevent further attempts to penetrate by implementing appropriate technical controls.
- **Monitor** critical points to ensure that the attacker does not continue.

Active Intrusions

There are two methods for dealing with an active hacker/cracker incident. The first method is to immediately lock the person out of the system and restore the system to a safe state. The second method is to allow the hacker/cracker to continue his probe/attack and attempt to gather information (forensics) that will lead to an identification and possible criminal conviction. The level of understanding of the risks involved and the knowledge of staff will determine the method used to handle a cracker/hacker incident. Under the direction of the FOCUS CIO, the following action will be taken:

- **Confirm** that the active session exists if possible. However, if doubt exists escalate to the next stage.
- **Contain** the hacker/cracker if the decision is to gather evidence and prosecute. If the decision is not to prosecute, contain the system at this stage to prevent further damage. Disconnection from the Internet is generally a first step. However, be careful to maintain all evidence. Everything you do can alter the system and destroy evidence. If necessary, create an image of the system to preserve the state of the system upon discovery.
- **Analyze** the system for evidence of the intrusion and the means used.
- **Eradicate** any traces of the attacker. If necessary, reinstall the entire operating system as it is not impossible that the attacker may have compromised system files and embedded a trap door for re-entry.
- **Recover** the system to the point where it can perform normal business functions again.
- **Review** the success of the handling of the incident. Determine the means of entry used and eliminate any vulnerability used by the hacker/cracker. Make modifications as necessary to the documented procedures.

Inactive Intrusions

In the case of where an incident is discovered after the fact, there is rarely a lot of evidence available to identify the perpetrator or how they gained access to the system. However, it is important that FOCUS adequately responds. The steps are basically the same as the active intrusion however time is not a critical factor and the quality of evidence is diminished. Under the direction of the FOCUS CIO, the following action will be taken:

- **Confirm** that the system experienced an intrusion in the past.
- **Contain** the system to prevent further damage and to preserve evidence. Disconnection from the Internet is generally a first step. If necessary, create an image of the system to preserve the state of the system upon discovery.
- **Analyze** the system for evidence of the intrusion and the means used.
- **Eradicate** any traces of the attacker. If necessary, reinstall the entire operating system, as it is not impossible that the attacker may have compromised system files and embedded a trap door for re-entry.
- **Recover** the system to the point where it can perform normal business functions again.
- **Review** the success of the handling of the incident. Determine the means of entry used and eliminate any vulnerability used by the hacker/cracker. Make modifications as necessary to the documented procedures.

Denial of Service or System Resources

Denials of service attacks affect the availability of system resources to legitimate users. However, the defense against denial of service attacks is difficult because it requires that FOCUS adequately identify legitimate versus illegitimate users. The procedures for mitigating a denial of service are to:

- Identify the source(s) of attack.
- Implement short-term technical controls to block attacker(s).

Virus, Worm, and Trojan Infection Procedures

Although virus and worm incidents are very different, the procedures for handling each are very similar aside from the initial isolation of the system and the time criticality. Viruses are not self-replicating and, therefore, incidents of this nature are not as time critical as worm or hacker incidents. Worms are self-replicating and can spread to hundreds of machines in a matter of minutes. Thus, time is a critical factor when dealing with a worm attack. If you are not sure of the type of the attack, proceed as if the attack was worm related. The following procedures are to be utilized infection is suspected:

- **Isolate** and contain the infected system(s) from the remaining FOCUS network as soon as possible. If a worm is suspected, then a decision must be made to disconnect the network from the outside world. Network isolation is one method to stop the spread of a worm, but the isolation can also hinder the clean-up effort since FOCUS will be disconnected from sites that may have patches. The FOCUS CIO must authorize the isolation of the FOCUS network from the outside world. Log all actions. **Do not power off or reboot systems that may be infected unless authorized to do so by the IT Department.** There are some viruses that will destroy disk data if the system is power-cycled or rebooted. Also, rebooting a system could destroy needed information or evidence.
- **Identify the source** of the problem Try to identify and isolate the suspected virus or worm-related files and processes. Prior to removing any files or killing any processes, a backup of the system should be made. If specific files that contain virus or worm code can be identified, then move those files to a safe place or archive them to tape and then remove the infected files. If other sites have been involved at this point, they may have helpful information on the problem and possible short-term solutions. Log all actions.
- **Contain** the virus or worm by suspending suspicious processes or applications. If the system is a Level 3 or Level 4 system make a full dump of the system and store in a safe place. The external hard disk drives should be carefully labeled so unsuspecting people will not use them in the future. Remove all suspected infected files or worm code. In the case of a worm attack, it may be necessary to keep the system(s) isolated from the outside world until all FOCUS systems have been inoculated and/or the other Internet sites have been cleaned up and inoculated. Log all actions.
- **Inoculate** the system(s) to prevent further infection by implementing fixes and/or patches to prevent further attack. Prior to implementing any fixes, it may be necessary to assess the level of damage to the system. If the virus or worm code has been analyzed, the task of assessing the damage is not very difficult. However, if the offending code has not been analyzed, it may be necessary to restore the system from external hard disk drive. Once the system is brought back into a safe mode, any patches or fixes should be implemented and tested. If possible, the virus or worm should be let loose on an isolated system that has been inoculated to ensure the system(s) are no longer vulnerable. Log all actions.

- **Return** to a normal operating mode. Prior to bringing the systems back into full operation mode, notify the same group of people who were notified in stage one. The users should also be notified that the systems are returning to a fully operational state. It may be wise to request all users to change their passwords. Before restoring connectivity to the outside world, verify that all affected parties have successfully eradicated the problem and inoculated their systems. Log all actions.
- **Follow-up** analysis should be performed to determine what allowed the breach in security that resulted in the infection.

Malware and Ransomware Procedures

Ransomware is no longer just an endpoint being encrypted by malware. Servers, applications and even data stored in cloud services can be encrypted and held for ransom. Although FOCUS maintains ransomware insurance coverage, FOCUS must be prepared with a comprehensive plan can help reduce the effects of any attack:

1. **Validate the attack.** The FOCUS CSO and IT Analysts shall confirm whether the event was indeed an attack. Many incidents can be linked to phishing, adware or other malware incidents but not specifically ransomware. If it is determined to be ransomware — i.e., files are encrypted or locked — proceed to the next steps.
2. **Gather the incident response team.** FOCUS shall ensure that IT Analysts, management, and legal teams are aware of the issue and ready to fulfill their roles in the response efforts.
3. **Analyze the incident.** The FOCUS CSO and IT Analysts shall examine the scope of the incident. The FOCUS CSO shall document which applications, networks and systems were affected, and determine how actively the malware is spreading.
4. **Contain the incident**. The FOCUS CSO and IT Analysts shall disconnect the infected system from the network to ensure the attack does not spread to other computers and devices and shall further ensure backups are secured and free of malware. Every incident will generate some volatile evidence, such as log files or system images. Document this evidence as soon as possible, and check it regularly, as it may change if the attack is ongoing. When ransomware is involved, such evidence may also include a recoverable encryption key as long as the investigation begins before the encryption key is deleted. In some cases, if the incident is detected quickly enough, the encryption can be stopped.
5. **Contact law enforcement.** The FOCUS CSO shall involve law enforcement agencies in the case of a high-impact incident or any/all data breach(es). Law enforcement experts may be able to offer guidance for paying ransoms based on previous experience with a strain of ransomware or criminal organization involved in the attack. FOCUS shall contact the Multi-State Information Sharing and Analysis Center, FBI or Internet Crime Complaint Center.
6. **Perform a thorough investigation.** The FOCUS CSO shall attempt to identify which ransomware strain has been used, its potential risks and recovery options. Some ransomware varieties use weak encryption that has a publicly available decryption mechanism provided by a security vendor or researcher. The No More Ransom initiative, a partnership between law enforcement and IT security companies, aims to help ransomware victims recover files where plausible.
7. **Eradicate malware, and recover from the incident.** The FOCUS CSO shall ensure that wiping infected systems and restoring lost data from backups is performed. All account, network and system passwords shall be changed after removing a device or system from the network. All passwords shall be changed again once the malware is removed completely from the network.
8. **Perform post-incident activities.** The FOCUS CSO shall adhere to regulatory and contractural breach notification requirements. The FOCUS CSO shall also verify the restoration of backups to ensure all applications, data and systems are accounted for.
9. **Perform analysis and learn from the attack.** During this step, the FOCUS CSO shall discover and analyze why the attack happened and apply appropriate actions to ensure the same vulnerability is not compromised in the future. For example, if the ransomware was the result of an employee clicking a malicious link, FOCUS shall perform additional security awareness training. Security policies shall be revised if necessary. The FOCUS CSO shall also analyze how the ransomware incident response plan performed and shall update the plan where needed to improve efficiency.

Security Incident Management Policy

FH Staff and peer reviewers are instructed to notify the FH Chief Security Officer or the Information Technology help desk with any known or suspected breaches of security or data loss, regardless of the breach being of an accidental nature or intentional. The FH Chief Security Officer shall evaluate each situation individually, assess the scope of the breach or loss, and initiate notifications in the matrix below within 7 business days of the suspected or actual breach:

Effected Client Companies	HHS if 500 or more	HHS if fewer than 500	Victims	Regulators
MSA instruction or Medical Director notified telephonically and via email, regardless of the size of the breach.	≥ 500 individuals, via weblink: https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf	< 500 individuals, via weblink: https://ocrportal.hhs.gov/ocr/breach/breach_form.jsf	CSO to review current rules/law and comply based on the latest requirements.	CSO to review current rules/law and comply based on the latest requirements.

POLICY:
Sanctions shall be fairly applied to employees following violations of the information security policies once a breach is verified and includes consideration of multiple factors. FOCUS documents personnel involved in incidents, steps taken, and the timeline associated with those steps, steps taken for notification, the rationale for discipline, and the final outcome for each incident. *1501.02f1Organizational.123* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Security Violations**'. Evidence of meeting this standard includes the requirement that the **FOCUS Code of Conduct** clearly stipulate sanctions in the event of confirmed and verified information security breaches, including consideration of multiple factors; and that an incident report is generated from within the FOCUS Review Management System in the **Security Incident** function; and that a **screenshot** is on file of this system; and that the report includes details regarding the employees involved, the incident, notifications, the rationale for discipline and the final outcome of each incident; and documentation of the incident shall be recorded in the permanent file of the employee. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, the inventory of security violations and their outcomes; and to record **meeting minutes** to document the findings and status of these security incidents. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the disciplinary process and determine whether sanctions for violations of the organizations security policies do not commence without prior verification of a breach. The formal disciplinary process ensures that correct and fair treatment for employees who are suspected of committing breaches of security and that a graduated response that takes into consideration factors (impact, number of offenses, training, regulatory requirements, and contractual obligations). And for each incident, the organization documents the personnel involved in the disciplinary process, the steps taken and the timeline associated with those steps, the steps taken for notification, the rationale for the discipline, whether the discipline was due to a compliance failure, and the final outcome.

PROCEDURES:
The FOCUS CSO ensures that:

- The formal sanctions policy and process is incorporated into the FOCUS Code of Conduct document, and is deployed within the FOCUS training system for all FOCUS Staff Members and Peer Reviewers to access, read and attest to complying with the policy & procedure upon initial hire and annually thereafter; and
- Upon awareness by any FOCUS Staff Member or contracted Peer Reviewer of suspected or actual non-compliance of FOCUS information security policies and procedures, the FOCUS staff member is required to notify the FOCUS Chief Security Officer (CSO) within one business day and report the suspected or actual infraction; and
- The FOCUS CSO is required to hold a FOCUS Administration meeting which must include at least two other senior staff members with all known information regarding alleged infractions by the Staff Member or Peer Reviewer; and
- The reporting mechanism to cite possible or actual infractions is to send an email to: compliance@focushm.com; and
- Upon agreement by FOCUS Administrators, the Chief Security Officer is to implement formal sanctions process upon the Staff Member or Peer Reviewer which initiated the infraction against FOCUS security policies and procedures as indicated below:

—

Sanctions
It is the policy of FOCUS Health, Inc. that all workforce members must protect the confidentiality, integrity, and availability of sensitive information at all times. FOCUS Health will categorize violations and impose sanctions, as described below, on any individual who accesses, uses, or discloses sensitive information without proper authorization. The sanctions will extend beyond protected health information that is in electronic form and include protected health information in written form.

FOCUS Health will take appropriate disciplinary action against employees, contractors, or any individuals who violate FOCUS Health's information security and privacy policies or state, or federal confidentiality laws or regulations, including the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH).

FOCUS Health has a rating system in place that is a reference for the appropriate personnel to utilize in addressing the disciplinary actions that should be taken according to the types of violations. The rating system is a three tier rating system and is composed of the following:

Level	Description of Violation
1	• Accessing information that you do not need to know to do your job. • Sharing computer access codes (user name & password). • Leaving computer unattended while being able to access sensitive information. • Disclosing sensitive information with unauthorized persons. • Copying sensitive information without authorization. • Changing sensitive information without authorization. • Discussing sensitive information in a public area or in an area where the public could overhear the conversation. • Discussing sensitive information with an unauthorized person. • Failing/refusing to cooperate with the Information Security Officer, and/or authorized designee. • Discarding PHI improperly (written) • Leaving PHI unprotected
2	• Second occurrence of any Level 1 offense (does not have to be the same offense). • Unauthorized use or disclosure of sensitive information. • Using another person's computer access code (user name & password). • Failing/refusing to comply with a remediation resolution or recommendation.
3	• Third occurrence of any Level 1 offense (does not have to be the same offense). • Second occurrence of any Level 2 offense (does not have to be the same offense). • Obtaining sensitive information under false pretenses. • Using and/or disclosing sensitive information for commercial advantage, personal gain, or malicious harm.

FOCUS Health, Inc. will utilize the following recommendations in determining the types of disciplinary actions to take when a violation occurs:

Violation Level	Recommended Disciplinary Action
1	• Verbal or written reprimand • Retraining on Security awareness • Retraining on Information Security policies • Retraining on the proper use of internal or required forms
2	• Letter of Reprimand; or suspension • Retraining on Security awareness • Retraining on Information Security policies • Retraining on the proper use of internal or required forms
3	• Termination of employment or contract • Administration’s discretion to report the incident to licensing boards, registration entities, and certification entities • Civil penalties as provided under HIPAA or other applicable Federal/State/Local law • Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law

Important Note: The recommended disciplinary actions are identified in order to provide guidance in policy enforcement and are not meant to be all-inclusive. When appropriate, progressive disciplinary action steps are to be followed allowing the employee to correct the behavior which caused the disciplinary action.

Exceptions: Depending on the severity of the violation, any single act may result in disciplinary action up to, and including termination of employment or contract with FOCUS Health, Inc.

MONITORING:

- It is the responsibility of the Chief Security Officer to:
    - Present this policy to FOCUS Administration for approval during annual or interim policy review meetings; and
    - Schedule annual review of this policy within the company calendar for monitoring; and
    - Provide access to all staff and contractors to report suspected or actual infractions to the CSO; and
    - Incoming email reports received by the CSO from compliance@focushm.com.

EVIDENCE:

- Meeting minutes, policy approval, policy distribution, policy attestations, personnel files, reported infraction log.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that a list of employees involved in security incidents is maintained with the resulting outcome from the investigation. *1502.02f1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the requirement that all employees involved in a security incident are documented within FOCUS Review Management System in the **Security Incident** function; and that a **screenshot** is on file of this system; and that the report includes details regarding the incident, employees involved, notifications, the rationale for discipline and the final outcome of each incident; and documentation of the incident shall be recorded in the permanent file of the employee. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, the inventory of security violations and their outcomes; and to record **meeting minutes** to document the findings and status of these security incidents. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— A list of employees involved in security incidents is maintained with the resulting outcome from the investigation; and
— Schedule a documented meeting upon reviewing the security incidents.

MONITORING:
- The FOCUS CSO reviews security incident documentation on a quarterly basis.

EVIDENCE:
- Meeting minutes, policy approval, personnel files, security incident report.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS Management shall approve the use of information assets and takes appropriate action when unauthorized activity occurs. *1504.06e1Organizational.34* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the requirement that FOCUS assess and deploy technologies to further monitor and ensure security policy compliance on the part of employees when unauthorized activity occurs. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, any additional technologies that have been deployed to monitor; and to record **meeting minutes** to document the findings and status of monitoring efforts. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to prevention of misuse of information to determine if management approves the use of information assets. If any unauthorized activity is identified by monitoring or other means, this activity is brought to the attention of the individual manager concerned for consideration of appropriate disciplinary and/or legal action.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— FOCUS Administrators are not to institute repercussions to anyone upon reporting another individual's violations.

MONITORING:
- The FOCUS CSO reviews security incident documentation on a quarterly basis.

EVIDENCE:
- Meeting minutes, policy approval, personnel files, security incident report.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that a formal security incident response program has been established to respond, report (without fear of repercussion), escalate and treat breaches and reported security events or incidents. FOCUS-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that should be included in the incident notification. This reporting includes notifying internal and external stakeholders, the appropriate community Computer Emergency Response Team, and law enforcement agencies in accordance with all legal or regulatory requirements for involving such organizations in computer incidents. *1505.11a1Organizational.13* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the establishment of a formal security incident response program to respond, report (without fear of repercussion), escalate and treat breaches and reported security events or incidents. Each FOCUS Staff member is required to read, understand and attest to the **FOCUS Code of Conduct** initially and annually thereafter; which clearly encourages reporting of suspected or actual security breaches, without repercussions; and stipulates sanctions in the event of confirmed and verified information security breaches, including consideration of multiple factors; and that an incident report is generated from within the FOCUS Review Management System in the **Security Incident** function; and that a **screenshot** is on file of this system. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, the inventory of security violations and their outcomes; and to record **meeting minutes** to document the findings and status of these security incidents. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the reporting of information security events to determine if formal information security event reporting procedures to support the corporate direction (policy) are established, together with an incident response and escalation procedure, setting out the action to be taken on receipt of a report of an information security event, treating the breach as discovered, and the timeliness of reporting and response. Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team, the mechanisms for such reporting, and the kind of information that is included in the incident notification. This reporting also includes notifying internal and external stakeholders, the appropriate Community Emergency Response Team and law enforcement agencies in accordance with all legal or regulatory requirements for involving that organization in computer incidents. With the importance of Information Security Incident Handling, a policy is established to set the direction of management. Employees and other workforce members, including third-parties, are able to freely report security weaknesses (real and perceived) without fear of repercussion.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Training is to be provided to FOCUS Employees and contracted Peer Reviewers, both initially and annually, regarding this policy and the Code of Conduct policy; and
— In addition to the policy ID 1501.02f1Organizational.123 above, explaining that FOCUS has a formal security incident response program established:
  • FOCUS Administrators are not to institute repercussions to anyone upon reporting another individual's violations; and
  • Organization-wide standards are specified for the time required for system administrators and other personnel to report anomalous events to the incident handling team as follows:
    • Upon any stakeholder reporting an anomalous event within the RMS, which must provide an on-screen form to categorize (classify) the nature of the incident, the name of the person reporting the anomaly, the date/time and a free-form note field for the reporter to provide details, and one-button access to read the segments of this policy relevant to reporting a security incident which includes a statement of 'No Repercussions' for reporting the incident; and
    • The CSO is to evaluate the nature of the incident and ensure, within one (1) hour that system security is in place and functional; and
    • The CSO is to call a meeting with FOCUS Administrators (CEO/CMO/CSO/COO/CFO) within three (3) business days to review the reported anomaly; and
    • The meeting is to be documented; and
    • Law enforcement agencies in accordance with all legal or regulatory requirements for involving such organizations in computer incidents are to be notified; and
    • All effected stakeholders are to be notified, both telephonically and via email, of the incident details.

MONITORING:
The FOCUS CSO monitors:
• Semi-annual review of service provider controls (policies & procedures) to ensure compliance; and
• Quarterly review of policies, inventory of security violations and their outcomes.

EVIDENCE:
• Meeting minutes, policy approval, personnel files, security incident reports.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

APPLICABLE SUPPORTING DOCUMENTS:

Location: RMS -> ADMIN -> ORGANIZATION -> SUPPORTING DOCUMENTS
FOCUS Code of Conduct

POLICY:
There shall be a point of contact for reporting information security events who is made known throughout FOCUS, always available, and able to provide adequate and timely response. FOCUS maintains a list of third-party contact information, which can be used to report a security incident. *1506.11a1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the requirement that FOCUS provides access to the CSO 24/7/365 for the reporting of security events via email address (compliance@focushm.com) or by telephone (727-647-8023 option 4); and a **screenshot** of this information available to all FOCUS Stakeholders is kept on file; and that a list of all FOCUS Vendors and their respective assigned security contact information shall be maintained in the **FOCUS Vendors function** of the FOCUS Review Management System. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies, confirmation of up-to-date vendor contacts and shall test the direct dial phone number and email system; and to record **meeting minutes** to document the findings and status of monitoring efforts. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Contact information for reporting incidents are to be within the FOCUS RMS incident response system; and
— Availability 24/7/365 is provided by the CSO to all stakeholders via telephone (727-647-8023 option 4) or via email at compliance@focushm.com; and
— The RMS provides a dedicated, on-screen form specifically designed to allow any stakeholder (FOCUS Employee, contracted Peer Reviewer, or Client-Company End user) to enter a percieved or actual incident and details they wish to share.
— If an email is received, response time to the transmitter of the email is to occur within four (4) hours; and
— The FOCUS RMS contains all contact information for vendors, client-companies, staff members and contract peer reviewers.

MONITORING:
The FOCUS CSO monitors:
• Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
• Meeting minutes, policy approval, screenshot of stakeholder contact information; screenshot of contact info within RMS incident response system.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall implemente an insider threat program that includes a cross-discipline insider threat incident handling team. *1507.11a1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the creation of the **FOCUS Insider Threat Program**; and that the FOCUS Chief Executive Officer, Chief Medical Officer, Chief Security Officer and Chief Operations Officer compose the insider threat incident handling team; and that the FOCUS Insider Threat Program procedures must be followed. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; hold documented (meeting minutes) quarterly meetings with the insider threat handling team to review policy, procedures and any recent threats. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
FOCUS Management ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— The incident management team that manages reported anomalies includes a cross-discipline handling team composed of FOCUS Administrators (CEO/CMO/CSO/COO/CFO/CCO); and
— Quarterly, documented meetings are to be held to review policies, threat handling procedures and review of past incidents.

MONITORING:
The FOCUS CSO monitors:
- Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, insider threat program administrative team.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The security incident response program shall account for and prepare FOCUS for a variety of incidents. *1516.11c1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the creation of the **FOCUS Insider Threat Program**; and that the program must address and prepare FOCUS for a variety of incidents. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS programs and policies, review the program's preparation of incidents, consider new threats or types of incidents to add to the program; and to record **meeting minutes** to document the findings and status of monitoring efforts. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the reporting and management of information security events to determine if the organization implements a formal incident response program, which includes the definition of specific phases for incident response. A program of business processes and technical measures are established to triage security-related events and handle different types of information security incidents including, system failure or loss of service, malicious code, denial of service, errors, unauthorized disclosures of covered information, system misuse, unauthorized wireless access points, and identity theft. In addition to normal contingency plans, the program also covers, analysis and identification of the cause of the incident, containment, increased monitoring of system use, planning and implementation of corrective action to prevent recurrence.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— The FOCUS Risk Assessments v 4.0 document is to include a wide variety of incidents and mitigation plans; and
— Incident response testing is to be conducted no less than annually; and
— Review of these risks are to include the incident management team to ensure completeness.

MONITORING:
The FOCUS CSO monitors:
- Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, FOCUS Risk Assessment inventory.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that there is a point of contact who is responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process. *1517.11c1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the appointment of the FOCUS Chief Security Officer to be the point of contact responsible for coordinating incident responses and has the authority to direct actions required in all phases of the incident response process. Further, in the absence of the CSO, the FOCUS Chief Executive Officer shall fulfill these duties. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Annually, the re-confirmation of the point of contact responsible for coordinating incident responses are to be documented within the RMS Administrative module.

MONITORING:
The FOCUS CSO monitors:
- Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, screenshot of RMS displaying the point of contact.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that workforce members cooperate with federal or state investigations or disciplinary proceedings. *1524.11a1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the incorporation of this requirement into the **FOCUS Code of Conduct** which clearly specifies that workforce members are to cooperate with federal or state investigations or disciplinary proceedings, and is attested to upon initial hire and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that all FOCUS Staff Members have attested FOCUS Code of Conduct documents on file and are current. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to security and privacy investigations and incident response, disciplinary actions, or other related topics to determine if organizations ensure that workforce members do not interfere with federal or state investigations or disciplinary proceedings through willful misrepresentation or omission of facts or by the use of threats or harassment against any person.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Workforce members cooperate with federal or state investigations or disciplinary proceedings; and
— Within the FOCUS Code of Conduct, FOCUS Employees and contract Peer Reviewers are to be trained and read/understand/attest and comply with this policy; and
— The FOCUS RMS incident submission screen is to indicate this information on-screen.

MONITORING:
The FOCUS CSO monitors:
- Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, training attestations; screenshot of RMS Incident Submission Screen.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall take disciplinary action against workforce members that fail to cooperate with federal and state investigations. *1525.11a1Organizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes policy which states that FOCUS takes disciplinary action against workforce members that fail to cooperate with federal and state investigations; and that this policy is included within the **FOCUS Code of Conduct**; and is attested to upon initial hire and annually thereafter. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that all FOCUS Staff Members have attested FOCUS Code of Conduct documents on file and are current. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— Training is provided to all FOCUS Employees and contracted Peer Reviewers to read/understand/attest and comply with this policy; and
— The FOCUS Code of Conduct includes disciplinary actions when non-compliance with investigators occurs; and
— FOCUS takes disciplinary action against workforce members that fail to cooperate with federal and state investigations by one or more of the following actions:
    - Termination of employment or contract; and/or
    - Administration's discretion to report the incident to licensing boards, registration entities, and certification entities; and/or
    - Civil penalties as provided under HIPAA or other applicable Federal/State/Local law; and/or
    - Criminal penalties as provided under HIPAA or other applicable Federal/State/Local law.

MONITORING:
The FOCUS CSO monitors:
- Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy. *1560.11d1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Security Violations**'. Evidence of meeting this standard includes quarterly review of all security incidents, and analysis by the FOCUS CSO for consideration of broadening the policies regarding incident response and recovery strategies. Further, the FOCUS CSO shall document, in meeting minutes, any findings and any proposed adjustments to the policy. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— This policy is reviewed at least quarterly to ensure compliance; and
— The information gained from the evaluation of information security incidents is used to identify recurring or high-impact incidents, and update the incident response and recovery strategy by:
• Incorporating incident evaluations into meetings with the CEO/CMO/CSO/COO/CFO so as to consider adding/modifying/deleting potential risks and mitigation plans regarding information security incidents.

MONITORING:
The FOCUS CSO monitors:
• Annual and Quarterly review of this policy and mechanisms to ensure compliance.

EVIDENCE:
• Meeting minutes, policy approval; modification/updating of the FOCUS Risk Assessment documentation.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure individuals are held accountable and responsible for actions initiated under their electronic signatures, to help deter record and signature falsification. *1581.02f1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that all FOCUS Staff Members have attested FOCUS Code of Conduct documents on file and are current. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that electronic signatures are prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— In the event FOCUS initiates use of electronic signatures, this policy is to be updated to include all applicable procedures, monitoring and evidence as needed to meet or exceed the HITRUST standard indicated above.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall tests and/or exercises its incident response capability regularly. 1589.11c1Organizational.5 This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes quarterly exercises conducted by the FOCUS CSO whereas a variety of hypothetical violations are discussed on a conference call with FOCUS IT Analysts; and the quarterly exercises are **documented** within meeting minutes by the CSO; and that any findings, ideas, concepts of potential improvement of FOCUS incident responses are documented and considered for integration into the FOCUS Security Policy and Procedure, Security Incident Response section. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS tests and/or exercises its incident response capability regularly by:
- Performing a simulation, solely with the participations of the incident response team, from reporting within the RMS incident response system to receiving the report, to conducting an incident response team meeting, to creating a mock report with hypothetical action items; and

— In the event any modifications to process are deemed appropriate, all relevant policies are to be updated to reflect the modifications.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes, policy approval, mock report example.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 15 INCIDENT MANAGEMENT

1501.02f1Organizational.123	HITRUST 02.f Disciplinary Process
1502.02f1Organizational.4	HITRUST 02.f Disciplinary Process
1504.06e1Organizational.34	HITRUST 06.e Prevention of Misuse of Information Assets
1505.11a1Organizational.13	HITRUST 11.a Reporting Information Security Events
1506.11a1Organizational.2	HITRUST 11.a Reporting Information Security Events
1507.11a1Organizational.4	HITRUST 11.a Reporting Information Security Events
1516.11c1Organizational.12	HITRUST 11.c Responsibilities and Procedures
1517.11c1Organizational.3	HITRUST 11.c Responsibilities and Procedures
1524.11a1Organizational.5	HITRUST 11.a Reporting Information Security Events
1525.11a1Organizational.6	HITRUST 11.a Reporting Information Security Events
1560.11d1Organizational.1	HITRUST 11.d Learning from Information Security Incidents
1581.02f1Organizational.7	HITRUST 02.f Disciplinary Process
1589.11c1Organizational.5	HITRUST 11.c Responsibilities and Procedures

Data Integrity Policy (back-ups and redundancy)

Backups in the primary (Tampa, FL) data center are performed on FH Servers every evening beginning at 12:00 AM ET. Backups take approximately 40 minutes to complete. These backups are executed to ensure data integrity in the event of hardware failures. The entire server hard disk set is backed up nightly 7 days per week.

(a) Backups are stored to disk.
(b) Backups are encrypted (using NIST FIPS 140-2 compliant encryption), catalogued and stored at a secondary data center location.
(c) Backup files are securely transported to the secondary data center location.
(d) Backups are retained for a defined period that meets client and regulatory requirements.
(e) Backup schedule and backup success is monitored to ensure backups are complete.
(f) Controls exist to ensure that transmitted backup data is processed securely, completely, and accurately.
(g) Backups of essential business-critical information are completed on a defined schedule.
(h) Backups of business application software are completed on defined schedule.
(i) Backup systems are available so that all essential business information and software can be recovered following a disaster or media failure.
(j) Restoration procedures are tested on a defined schedule to ensure they are effective and can be completed within the time allotted in the operational procedures for recovery.
(k) Procedures are enforced which establish retention periods for essential business information.
(l) Procedures are enforced which establish requirements for permanent retention of archive copies.
(m) In the event that hardware and electronic media containing PHI/PII, the item(s) are identified and tracked during movement.

The primary data center additionally securely posts transactional changes to a live, duplicate copy of the fully functioning production system to the secondary (Atlanta, GA) data center every 5 minutes. This process provides the ability for FH to 'failover' to the secondary data center in the event that the primary is rendered unusable for any reason. The secondary data center is fully functional and provides access to all stakeholders (FH Employees, FH Peer Reviewers, and Client-Company Care Managers). If a failure occurs in the primary data center, the secondary data center is to be accessible within minutes.

POLICY:
FOCUS shall implement a business continuity plan for program operations, including information system(s) (*electronic* and paper) that: *URAC C14* (No Weight)

(a) Identifies which systems and processes must be maintained and the effect an outage would have on the *organization's* program; (3)
(b) Identifies how business continuity is maintained given various lengths of time information systems are not functioning or accessible; (3)
(c) Is tested at least every two years; **and** (3)
(d) Responds promptly to detected problems and takes corrective action as needed. (3)

These URAC standards are implemented within the **FOCUS Business Continuity and Disaster Recovery Plan**[(a)(b)(c)]. Measurement of success is based on the creation, maintenance, and accurate execution of these FOCUS Policies and procedures; and identifies systems and processes which must be maintained and the effect an outage would have on FOCUS' Programs; and Identifies how business continuity is maintained given various lengths of time information system are not functioning or accessible; and is tested annually; and FOCUS must respond promptly to detected problems and takes corrective action as needed; and other evidence as documented in committee meetings. Ongoing quality assurance monitoring mechanisms include annual review of the programs, policies and procedures, and ongoing monitoring of reports and logs with quarterly committee meetings. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
Please refer to the document entitled 'FH Disaster Recovery Business Continuity Plan v 13.1' (DR/BCP)
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS tests the DR/BCP by:
  • Performing simulations, as documented in the FOCUS Disaster Recovery / Business Continuity Plan; and
— In the event any modifications to process are deemed appropriate, all relevant policies are to be updated to reflect the modifications.

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Annual review of the DR/BCP tests are to be conducted with opportunity to refine testing process.

EVIDENCE:
• Meeting minutes, policy approval, DR/BCP testing results.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that the Company can recover and restore business operations and establish an availability of information in the time frame required by the business objectives and without a deterioration of the security measures. *1601.12c1Organizational.1238* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery Policy**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Policy**; and testing to be conducted annually with the **FOCUS Disaster Recovery Test**, which creates a report to be stored within the FOCUS Review Management System supporting documents function; and subsequent analysis of the test so as to refine and improve policies and procedures to meet established goals and objectives of recuperation in the event of an interruption of services to FOCUS client-companies. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; hold documented (meeting minutes) quarterly meetings with the FOCUS IT Analysts to review outcomes of tests to make recommendations to optimize policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to business continuity to determine if the business continuity planning process includes the following: (i) recovery and restoration of business operations and establish an availability of information in a time-frame specified by the organization; (ii) particular attention is given to the assessment of internal and external business dependencies and the contracts in place; (iii) documentation of agreed procedures and processes; and, (iv) testing and updating of at least a section of the plans.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS can recover and restore business operations and establish an availability of information in the time frame required by the business objectives and without a deterioration of the security measures, by:
- Establishing the Disaster Recovery and Business Continuity Plan; and
- Testing the plan no less than annually; and
- Refining and improving the plan based on results of testing, changes in the environment, changes in security technology and requirements, staff training, redundancy and education.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Annual review of the DR/BCP tests are to be conducted with opportunity to refine testing process.

EVIDENCE:
- Meeting minutes, policy approval, DR/BCP testing results.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

APPLICABLE SUPPORTING DOCUMENTS:
Location: RMS -> ADMIN -> ORGANIZATION -> SUPPORTING DOCUMENTS
FOCUS Disaster Recovery Test

POLICY:
FOCUS shall ensure that the contingency program addresses required capacity, identifies critical missions and business functions, defines recovery objectives and priorities, and identifies roles and responsibilities. *1602.12c1Organizational.4567* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan**; and testing to be conducted annually with the **FOCUS Disaster Recovery Test**, which creates a report to be stored within the FOCUS Review Management System supporting documents function; and analysis of test results that addresses required capacity, identifies critical missions and business functions, defines recovery objectives and priorities, and identifies roles and responsibilities. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies to ensure accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to business continuity to determine if developed business continuity plans: (i) identify the necessary capacity for information processing, telecommunications, and environmental support is available during contingency operations, e.g., during an information system disruption, compromise or failure; (ii) identify essential missions and business functions and associated contingency requirements; (iii) provide recovery objectives, restoration priorities, and metrics; and, (iv) address contingency roles, responsibilities, and assign individuals with contact information.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— FOCUS The contingency program addresses required capacity, identifies critical missions and business functions, defines recovery objectives and priorities, and identifies roles and responsibilities.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Annual review of the DR/BCP tests are to be conducted with opportunity to refine testing process.

EVIDENCE:
- Meeting minutes, policy approval.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

APPLICABLE SUPPORTING DOCUMENTS:
Location: RMS -> ADMIN -> ORGANIZATION -> SUPPORTING DOCUMENTS
FOCUS Disaster Recovery Test

POLICY:
FOCUS shall ensure that copies of the business continuity plans are distributed to key contingency personnel. *1603.12c1Organizational.9* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery Policy**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Policy**, which shall be available 24/7/365 within the FOCUS Review Management System and also distributed via email monthly in the form of a password protected and encrypted PDF file to key contingency personnel. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format as well. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that monthly distribution to key personnel has been accomplished. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Copies of the business continuity plans are distributed to key contingency personnel.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Annual review of the DR/BCP tests are to be conducted with opportunity to refine testing process.

EVIDENCE:
- Meeting minutes, policy approval.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

POLICY:
FOCUS shall ensure that backup copies of information and software are made and tests of the media and restoration procedures are regularly performed at appropriate intervals. *1616.09l1Organizational.16* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan**, which stipulates that backup copies of information and software are made and tests of the media and restoration procedures are regularly performed at appropriate intervals. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format as well. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to backup of data and determine if back-up copies of information and software are be made, and when equipment is moved (relocated), and tested regularly, in accordance with an agreed-upon back-up policy. Regular testing of back-up media and restoration procedures performed.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Backup copies of information and software are made and tests of the media and restoration procedures are regularly performed at appropriate intervals by:
  - Instructing the FOCUS IT Analysts to ensure that the RMS Server automated backup routine is checked on a daily basis via confirmation of auto-generated server email notification regarding successful backup to ensure backups are being made; and
  - Randomly launching 3 of the files, on a weekly basis, which have been backed up to ensure file integrity; and
  - Testing of the restoration procedures are performed quarterly to ensure that the backup files, process and software work effectively and properly; and

— Testing is documented within the RMS Administrator module

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Backup logs and file integrity reports authored by FOCUS IT Analysts.

EVIDENCE:
- Meeting minutes; policy approval; backup logs; file integrity reports.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

POLICY:
FOCUS shall ensure that a formal definition of the level of backup required for each system is defined and documented including how each system will be restored, the scope of data to be imaged, frequency of imaging, and duration of retention based on relevant contractual, legal, regulatory and business requirements. *1617.09l1Organizational.23* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan.** Further evidence shall be on file of the Business Continuity and Disaster Recovery Plan in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— A formal definition of the level of backup required for each system is defined and documented:
- Data Center Systems: Each system is to be backed up utilizing the integrated software within MacOS known as 'Time Machine' to a centralized 'Time Machine' server with a large enough drive to store numerous independent systems within the data center. This automated backup tool encrypts all files and backs up hourly (for 24 hours); daily (for 30 days); and weekly backups for all previous months. The oldest backups are deleted if the drive becomes full. This system also backs up the virtual desktops housed within the data center for FOCUS Employees to remotely access, thereby keeping all covered data within the data center. Backup data is included and applicable to the FOCUS data retention policy.

— Immediate access to system logs (ASA, RMS, Operating Systems) are to be retained for a minimum of 90 days.

— A formal definition including how each system will be restored:
- Time Machine provides the ability to restore a whole drive or individual files with ease; therefore, in the event of a minor loss of files - or a whole drive - Time Machine decrypts the backed up files and installs them into their original positions on the originating computer when directed.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Backup logs and file integrity reports authored by FOCUS IT Analysts.

EVIDENCE:
- Meeting minutes; policy approval; backup logs; file integrity reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

POLICY:
FOCUS shall ensure that backups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location. *1618.09I1Organizational.45* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan**, which stipulates that the backups are stored in a physically secure remote location, at a sufficient distance to make them reasonably immune from damage to data at the primary site, and reasonable physical and environmental controls are in place to ensure their protection at the remote location. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format as well. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Hard disk drives are to be the target devices to store backups (not tape drives); and
— Backups are to be stored within the FOCUS secure data cabinet; but at a sufficient distance to make them reasonably immune from damage to data at the primary site; and
— Reasonable physical and environmental controls are in place to ensure their protection at the remote location (e.g., the data center with certifications for all safety and security certifications thereof.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Backup logs and file integrity reports authored by FOCUS IT Analysts; and
- Data center safety and security certifications.

EVIDENCE:
- Meeting minutes; policy approval; data center safety and security certifications.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that inventory records for backup copies, including content and current location, are maintained. *1619.09l1Organizational.7*
This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Business Continuity and Disaster Recovery**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan**, which stipulates that Inventory records for the backup copies, including content and current location, are maintained. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format; and **screenshots** of the FOCUS Review Management System Systems Inventory Function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies to ensure accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Inventory records for the backup copies, including content and current location, are maintained by:
  • FOCUS IT Analysts entering backup inventory location information into the RMS Administration module/IT Inventory system.

MONITORING:
The FOCUS CSO monitors:
  • Annual review of this policy and mechanisms to ensure compliance; and
  • Backup inventory reports authored by FOCUS IT Analysts.

EVIDENCE:
  • Meeting minutes; policy approval; backup inventory reports.

RESPONSIBLE PARTY:
  • FOCUS IT Analyst

POLICY:
FOCUS shall ensure that when backup service is delivered by the third party, the service level agreement includes the detailed protections to control confidentiality, integrity and availability of the backup information. *1620.09l1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Plan**, which stipulates that FOCUS shall not engage in outsourcing of a third party backup service for any FOCUS data. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format; and **screenshots** of the FOCUS Review Management System Systems Inventory Function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that at no time will a third party be contracted with or provide services to backup any FOCUS data, including covered data.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— In the event the need to acquire a third party backup service, this policy is to be modified to fulfill the HITRUST standard above, and approved by FOCUS Administration (CEO/CMO/CSO/COO/CFO/CCO).

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approval.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall identify the critical business processes requiring business continuity.[1634.12b1Organizational.1] This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FH Disaster Recovery Business Continuity Plan**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the FH Disaster Recovery Business Continuity Plan, which stipulates that FOCUS shall identify the critical business processes requiring business continuity. Further evidence shall be on file of **screenshots** of the Business Continuity and Disaster Recovery Plan; and the Business Continuity and Disaster Recovery Plan in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— Business Continuity Planning (BCP) is an interdisciplinary concept used to create and validate a practiced logistical plan for how FOCUS Health will recover and restore partially or completely interrupted critical function(s) within a predetermined time after a disaster extended disruption. The logistical plan is called a *Business Continuity Plan; and*
— In plain language, BCP is working out how to stay in business in the event of disaster. Disasters include local incidents like building fires, regional incidents like earthquakes, or national incidents like pandemic illnesses.
BCP is a part of an organizational learning effort that helps reduce operational risk associated with lax information management controls. This process may be integrated with improving information security and corporate reputation risk management practices.
— The following matrix illustrates the prioritization of service restoration in the event of a catastrophe:

System	Prioritization	Restoration Objective
FOCUS Review Management System	1	100%
VoIP Telephone System	2	100%
Electronic Mail System	3	100%
Teams Chat System	4	100%

— FOCUS is dedicated to maintaining access to the online Review Management System 24 hours per day, 365 days per year. To that end, technologies and environmental challenges must be identified and overcome, while retaining security of data at all times; and
— For all details regarding BCP, please refer to 'FH Disaster Recovery Business Continuity Plan.pdf".

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance.

EVIDENCE:
• Meeting minutes; policy approval.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy

POLICY:
FOCUS shall ensure that information security aspects of business continuity are (i) based on identifying events (or sequence of events) that can cause interruptions to FOCUS's critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters acts of terrorism); (ii) followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period; (iii) based on the results of the risk assessment, a business continuity strategy is developed to identify the overall approach to business continuity; and (iv) once this strategy has been created, endorsement is provided by management, and a plan created and endorsed to implement this strategy. *1635.12b1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**FH Disaster Recovery Business Continuity Plan v 13.1.pdf**' and **Risk Assessments v 4.0.pdf.** Evidence of meeting this standard includes creation and maintenance of the two aforementioned documents, conducted annually. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the business continuity management process to determine if information security aspects of business continuity are: (i) based on identifying events (or sequence of events) that can cause interruptions to the organizations critical business processes (e.g., equipment failure, human errors, theft, fire, natural disasters and acts of terrorism); (ii) followed by a risk assessment to determine the probability and impact of such interruptions, in terms of time, damage scale and recovery period; (iii) based on the results of the risk assessment, a business continuity strategy is developed to identify the overall approach to business continuity; and, (iv) once this strategy has been created, endorsement is provided by management, and a plan created and endorsed to implement this strategy.

PROCEDURES:
The FOCUS CSO ensures that:
— These policies are reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are to be provided training on both aforementioned documents to read/understand/attest and comply with the policies.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

APPLICABLE POLICIES:
Location: RMS -> ADMIN -> ORGANIZATION -> P&Ps
Business Continuity and Disaster Recovery Policy
Risk Asessment Policy

POLICY:
FOCUS shall create, at a minimum, one (1) business continuity plan and ensures each plan (i) has an owner, (ii) describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security, and (iii) specifies the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan. *1666.12d1Organizational.1235* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**FH Disaster Recovery Business Continuity Policy**'. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Business Continuity and Disaster Recovery Policy.** Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies for accuracy and completeness. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the business continuity management to determine if the organization creates at a minimum one business continuity plan and ensures each plan (i) has an owner, (ii) describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security, and (iii) specifies the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan.

PROCEDURES:
The FOCUS CSO ensures that:
— The Disaster Recovery / Business Continuity policy is reviewed/modified/ratified no less than annually; and
— The FOCUS IT Analysts are to be provided training on both aforementioned document to read/understand/attest and comply with the policies; and
— The plan (i) has an owner, (ii) describes the approach for continuity, ensuring at a minimum the approach to maintain information or information asset availability and security, and (iii) specifies the escalation plan and the conditions for its activation, as well as the individuals responsible for executing each component of the plan.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Review the Disaster Recovery / Business Continuity policy on a quarterly basis to ensure modernization and optimization by proposing interim updates, if necessary; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Disaster Recovery Business Continuity Policy

POLICY:
FOCUS shall ensure that when new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) are amended as appropriate. *1667.12d1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FH Disaster Recovery Business Continuity Policy**'. Evidence of meeting this standard includes the review of the plan on a quarterly basis. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— The FOCUS Disaster Recovery Business Continuity Policy is reviewed/modified/ratified no less than annually; and
— When new requirements are identified, any existing emergency procedures (e.g., evacuation plans or fallback arrangements) are amended as appropriate by:
  - Reviewing the plan on a quarterly basis, and adding/modifying/deleting from the plan as needed, followed by presentation to the FOCUS Administrative team (CEO/CMO/CSO/COO/CFO) for finalization, ratification, activating (effective date) followed by distribution and instruction to applicable stakeholders.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Review of the FOCUS Disaster Recovery Business Continuity Policy on a quarterly basis to ensure modernization and optimization by proposing interim updates, if necessary; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; training attestations.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Disaster Recovery Business Continuity Policy

POLICY:
FOCUS shall ensure that emergency procedures, manual "fallback" procedures, and resumption plans are the responsibility of the owner of the business resources or processes involved; and fallback arrangements for alternative technical services, such as information processing and communications facilities, are the responsibility of the service providers. *1668.12d1Organizational.67* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FH Disaster Recovery Business Continuity Policy**'. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— The FOCUS Disaster Recovery Business Continuity Policy is reviewed/modified/ratified no less than annually; and
— Emergency procedures, manual "fallback" procedures, and resumption plans are the responsibility of the owner of the business resources or processes involved. For FOCUS, this is the CSO/CSO.
— Fallback arrangements for alternative technical services, such as information processing and communications facilities, are the responsibility of the service providers.

MONITORING:
The FOCUS CSO monitosr:
- Annual review of this policy and mechanisms to ensure compliance; and
- The aforementioned policy on a quarterly basis to ensure modernization and optimization by proposing interim updates, if necessary; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Disaster Recovery Business Continuity Policy

POLICY:
FOCUS shall ensure that the business continuity planning framework addresses a specific, minimal set of information security requirements. *1669.12d1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**FH Disaster Recovery Business Continuity Policy**'. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the business continuity management to determine if the business continuity planning framework addresses the identified information security requirements, including the following: (i) the conditions for activating the plans which describe the process to be followed (e.g., how to assess the situation, who is to be involved) before each plan is activated; (ii) emergency procedures which describe the actions to be taken following an incident that jeopardizes business operations; (iii) fallback procedures which describe the actions to be taken to move essential business activities or support services to alternative temporary locations, and to bring business processes back into operation in the required time-scales; (iv) resumption procedures which describe the actions to be taken to return to normal business operations; (v) a maintenance schedule which specifies how and when the plan will be tested, and the process for maintaining the plan; (vi) awareness, education, and training activities which are designed to create understanding of the business continuity processes and ensure that the processes continue to be effective; and, (vii) the critical assets and resources needed to be able to perform the emergency, fallback and resumption procedures.

PROCEDURES:
The FOCUS CSO ensures that:
— The FOCUS Disaster Recovery Business Continuity Policy policy is reviewed/modified/ratified no less than annually; and
— The business continuity planning framework addresses a specific, minimal set of information security requirements by:
  • Clearly indicating the minimal set of information security requirements, as indicated in the FH Disaster Recovery Business Continuity Plan.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- The FOCUS Disaster Recovery Business Continuity Policy on a quarterly basis to ensure modernization and optimization by proposing interim updates, if necessary; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Disaster Recovery Business Continuity Policy

POLICY:
FOCUS shall ensure that workforce members roles and responsibilities in the data backup process are identified and communicated to the workforce; in particular, Bring Your Own Device (BYOD) users are required to perform backups of organizational and/or client data on their devices. *1699.09l1Organizational.10* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that it is strictly prohibited for end-users (including BYOD users) to download, backup, record, store or print any FOCUS data at any time.

PROCEDURES:
The FOCUS CSO ensures that:
— The aforementioned policy is reviewed/modified/ratified no less than annually; and
— Training is to be provided to FOCUS Staff Members and contracted Peer Reviewers so that they read/understand/attest and comply with this policy; and
— Due to the informational architecture (remote sessions served from our data center) and company-owned hardware that FOCUS provides Employees, workforce members roles and responsibilities in the data backup process are non-existent and prohibited; and
— Due to the informational architecture (web services served from our data center) that FOCUS provides contracted Peer Reviewers, Peer Reviewer roles and responsibilities in the data backup process are non-existent and prohibited.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- This policy on a quarterly basis to ensure modernization and optimization by proposing interim updates, if necessary; and
- Training logs to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; training logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 16 BUSINESS CONTINUITY AND DISASTER RECOVERY

URAC C14	URAC CORE 14: Business Continuity
1601.12c1Organizational.1238	HITRUST 12.c Developing and Implementing Continuity Plans Including Information Security
1602.12c1Organizational.4567	HITRUST 12.c Developing and Implementing Continuity Plans Including Information Security
1603.12c1Organizational.9	HITRUST 12.c Developing and Implementing Continuity Plans Including Information Security
1616.09l1Organizational.16	HITRUST 09.l Back-up
1617.09l1Organizational.23	HITRUST 09.l Back-up
1618.09l1Organizational.45	HITRUST 09.l Back-up
1619.09l1Organizational.7	HITRUST 09.l Back-up
1620.09l1Organizational.8	HITRUST 09.l Back-up
1634.12b1Organizational.1	HITRUST 12.b Business Continuity and Risk Assessment
1635.12b1Organizational.2	HITRUST 12.b Business Continuity and Risk Assessment
1666.12d1Organizational.1235	HITRUST 12.d Business Continuity Planning Framework
1667.12d1Organizational.4	HITRUST 12.d Business Continuity Planning Framework
1668.12d1Organizational.67	HITRUST 12.d Business Continuity Planning Framework
1669.12d1Organizational.8	HITRUST 12.d Business Continuity Planning Framework
1699.09l1Organizational.10	HITRUST 09.l Back-up

17 Risk Management

POLICY:
FOCUS shall perform risk assessments in a consistent way and at planned intervals, or when there are major changes to FOCUS's environment, and reviews the risk assessment results annually. *1704.03b1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments v 4.0.pdf'**. Evidence of meeting this standard includes the creation and ongoing maintenance of the **FOCUS Risk Assessment** document, which stipulates that FOCUS performs thorough risk assessments in a consistent way and at annual intervals, or when there are major changes to FOCUS's environment, and reviews the risk assessment results annually. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to performing risk assessments to determine whether risk assessments are performed that address all the major domains of the HITRUST CSF. Risk assessments are consistent and identify information security risks to the organization. Risk assessments are to be performed at planned intervals, or when major changes occur in the environment, and the results reviewed annually.

If changes to FOCUS systems are being considered, or any change may impact security, a risk assessment shall be conducted as FOCUS integrates Risk Management and Change Management functions.

PROCEDURES:
The FOCUS CSO ensures that:
— The 'Risk Assessments' document and this policy is reviewed/modified/ratified no less than annually; and
— A documented annual meeting with the FOCUS IT Analysts and the FOCUS Administrative team to review/add/modify/delete elements as needed to the 'Risk Assessments' document to ensure that all company, environmental and stakeholder risks are identified and documented; and
— If there are any major changes to the FOCUS environment (business or IT related changes), FOCUS is to hold a documented ad-hoc meeting with the FOCUS IT Analysts and FOCUS Administrative team to review/add/modify/delete elements as needed to he 'Risk Assessments' document to ensure that all company, environmental and stakeholder risks are identified and documented; and
— In the event an emergency change is requested, the change request is fully documented and management approval is required.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly meetings held with the FOCUS IT Analysts to identify any IT/architectural related changes that would warrant ad-hoc review of the 'Risk Assessments' document.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Risk Assessments

POLICY:
FOCUS shall use a formal methodology with defined criteria for determining risk treatments and ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented. *1707.03c1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments v 4.0.pdf**'. Evidence is to be on file of the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to risk mitigation to determine whether the organization has defined criteria to determine an appropriate risk treatment (e.g., accept, mitigate, transfer or avoid) that include industry or organizational laws, regulations or standards, contractual, business or other priorities, cultural fit, customer/client concerns, IT policy and strategies, risk and business strategies, cost, effectiveness, type of protection, threats covered, risk levels, existing alternatives and additional benefits derived from the risk treatment. Further, the organization implements a process for ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained; and the remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented.

PROCEDURES:
The FOCUS CSO ensures that:
— The 'Risk Assessments' document and this policy is reviewed/modified/ratified no less than annually; and
— A formal methodology with defined criteria for determining risk treatments and ensuring that corrective action plans for the security program and the associated organizational information systems are prioritized and maintained, by:
  • Scope; and
  • Definitions; and
  • Risk Assessment Deliverables; and
  • Risk Assessment Requirements; and
  • Risk Assessment Methods; and
  • Accountable parties; and
  • Risk Assessment Steps
  • Risk Assessment Findings; and
  • Risk Assessment Vulnerabilities; and
  • Acceptable Risks
  • Required Back-Out Plan
— The remedial information security actions necessary to mitigate risk to organizational operations and assets, individuals, and other organizations are documented by:
  • Risk Mitigation; and
  • Enforcement

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Quarterly policy review.

EVIDENCE:
• Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

REFERENCED POLICY:
• FOCUS Risk Assessments

POLICY:
FOCUS shall ensure that risk assessments include the evaluation of multiple factors that may impact security as well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems. *1706.03b1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments v 4.0.pdf**'. Evidence of meeting this standard includes the stipulation that risk assessments include the evaluation of multiple factors that may impact security as well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems. Further evidence shall be on file of **screenshots** of the FOCUS Risk Assessment document; and the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to performing risk assessments to determine whether the risk assessment–used to validate a breach of unsecured Protected Health Information (PHI), as these terms are defined by the Secretary of Health and Human Services is reportable to the Secretary–demonstrates there is a low probability of compromise (lo pro co), rather than a significant risk of harm.

PROCEDURES:
The FOCUS CSO ensures that:
— The 'Risk Assessments' document and this policy is reviewed/modified/ratified no less than annually; and
— Risk assessments include the evaluation of multiple factors that may impact security as well as the likelihood and impact from a loss of confidentiality, integrity and availability of information and systems (please see 'Risk Assessment' document for details); and
— A documented quarterly meeting when the CSO reviews the policy is to be made.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly policy review.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Risk Assessments

POLICY:
FOCUS shall mitigate any harmful effect that is known to FOCUS of a use or disclosure of PHI by FOCUS or its business associates, in violation of its policies and procedures. *1713.03c1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the stipulation that FOCUS mitigates any harmful effect that is known to FOCUS of a use or disclosure of PHI by FOCUS or its business associates, in violation of its policies and procedures. Further evidence shall be on file of **screenshots** of the FOCUS Risk Assessment document; and the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS mitigates any harmful effect that is known to FOCUS of a use or disclosure of PHI by FOCUS or its business associates, in violation of its policies and procedures by:
- Identifying client-companies effected and based on contractural requirements and SLAs (Service Level Agreements), FOCUS is to take steps, within designated notification instructions per client-company, to notify of PHI disclosure(s) in detail; and
- The CSO is to take steps to initiate mitigation steps (hardware/software/policies/procedures) to prevent further disclosure of PHI; and
- Based on monthly (up-to-date) compliance research and findings, the FOCUS Administrative team is to notify all required Federal and/or State entities as required by law; and
- Initiating a documented investigation to identify who/what/where/when/why/how any harmful effect occurred; and
- Following FOCUS policies (above) regarding actions to be taken if a violation has occurred against the disclosing party.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Monthly compliance research to ensure that FOCUS responsibilities in reporting a disclosure of PHI are followed; and
- Quarterly policy review.

EVIDENCE:
- Meeting minutes; policy approvals; PHI disclosure report.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The FOCUS risk management program shall include the requirement that risk assessments be re-evaluated at least annually, or when there are significant changes in the environment. *1733.03d1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments v 4.0.pdf**'. Evidence of meeting this standard includes the stipulation that the risk management program includes the requirement that risk assessments be re-evaluated at least annually, or when there are significant changes in the environment. Further evidence shall be on file the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; or
— When there are significant changes in the environment; and
— A documented quarterly meeting is held demonstrating review and assessment of the existing policy to ensure optimization.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall formally address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements and facilitates the implementation of system and information integrity requirements/controls. *1780.10a1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments**'. Evidence of meeting this standard includes the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance with system and information integrity requirements; and
— Facilitates the implementation of system and information integrity requirements/controls.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Risk Assessments

POLICY:
FOCUS shall ensure that information system specifications for security control requirements state that security controls are to be incorporated in the information system, supplemented by manual controls as needed, and these considerations are also applied when evaluating software packages, developed or purchased. *1781.10a1Organizational.23* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments**'. Evidence of meeting this standard includes the stipulation that Information system specifications for security control requirements state that security controls are to be incorporated in the information system, supplemented by manual controls as needed, and these considerations are also applied when evaluating software packages, developed or purchased. Further evidence shall be on file of **screenshots** of the FOCUS Risk Assessment document; and the FOCUS Risk Assessment in PDF format; and **screenshots** of the FOCUS Review Management System Change Request Function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Information system specifications for security control requirements state that security controls are to be incorporated in the information system, supplemented by manual controls as needed, and these considerations are also applied when evaluating software packages, developed or purchased.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Risk Assessments

POLICY:
FOCUS shall ensure that security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security. *1782.10a1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Risk Assessments**'. Evidence of meeting this standard includes the FOCUS Risk Assessment in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Security requirements and controls reflect the business value of the information assets involved, and the potential business damage that might result from a failure or absence of security.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- FOCUS Risk Assessments

POLICY:
FOCUS shall ensure that a formal acquisition process is followed for purchased commercial products, and supplier contracts include the identified security requirements. *1783.10a1Organizational.56* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and **screenshots** of the FOCUS Review Management System IT Request System. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities are to be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— A formal acquisition process is followed for purchased commercial products, and supplier contracts include the identified security requirements by:
• The FOCUS RMS Is to provide a venue so that IT related requests can be entered; and
• The CSO assesses the request against current budget allowances; and
• If accepted, the CSO engages the FOCUS IT Analysts to acquire cost and availability estimates and possible alternatives; and
• The CSO then approves the request, where FOCUS IT Analysts is to place the order, track the order and ensure testing and configuration of the hardware/software and assess security concerns and risks; and
• The CSO then approves the implementation as documented in the RMS Administration module/IT Inventory system; and
• The FOCUS IT Analysts is to monitor the new hardware/software for thirty (30) days to ensure security and function.

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Quarterly review to ensure compliance.

EVIDENCE:
• Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls are reconsidered prior to purchasing the product. *1784.10a1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Acquisitions**'. Evidence of meeting this standard includes the stipulation that where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls are reconsidered prior to purchasing the product. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and **screenshots** of the FOCUS Review Management System Change Request Function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Where the security functionality in a proposed product does not satisfy the specified requirement, the risk introduced and associated controls are reconsidered prior to purchasing the product by:
- The FOCUS CSO is to reconsider the request in whole, to prioritize security first; and
- If deemed worthy of additional research and testing, the CSO is to instruct the FOCUS IT Analysts to proceed with research for acceptable, security-capable alternatives; and
- If an alternative is found, acquisition is granted and security testing is to commence in a testing environment; and
- Upon confirmation that security is not compromised, the hardware/software is to be installed for use by the requestor; and
- Testing in the production environment is conducted, and if approved, the FOCUS IT Analysts are to monitor the new hardware/software for a period of thirty (30) days to ensure continual security acceptability.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that where additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls. *1785.10a1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Acquisitions**'. Evidence of meeting this standard includes the stipulation that where additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls; and that there shall be no default account in new devices; and that unnecessary features or functions of new devices are disabled. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and **screenshots** of the FOCUS Security Appliance (firewall) configuration tool. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Where additional functionality is supplied and causes a security risk, the functionality is disabled or mitigated through application of additional controls by:
  - The FOCUS CSO is to instruct the FOCUS IT Analysts to disable the additional functionality immediately upon knowledge that security is (or could be) compromised; and
  - The FOCUS CSO is to reconsider the request in whole, to prioritize security first; and
  - If deemed worthy of additional research and testing, the CSO is to instruct the FOCUS IT Analysts to proceed with research for acceptable, security-capable alternatives; and
  - If an alternative is found, acquisition is granted and security testing is to commence in a testing environment; and
  - Upon confirmation that security is not compromised, the hardware/software is to be installed for use by the requestor; and
  - Testing in the production environment is conducted, and if approved, the FOCUS IT Analysts are to monitor the new hardware/software for a period of thirty (30) days to ensure continual security acceptability.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall require developers of information systems, components, and developers or providers of services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use. *1786.10a1Organizational.9*
This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Software Development Life Cycle**'. Evidence of meeting this standard includes the Software Development Life Cycle V 6.0.pdf document. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: As of the Effective Date of this policy, FOCUS does not develop software, write 'code' nor compile application code.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS requires developers of information systems, components, and developers or providers of services to identify (document) early in the system development life cycle, the functions ports, protocols, and services intended for organizational use.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Software Development Life Cycle

POLICY:
FOCUS shall implement an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks. *17126.03c1System.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Risk Assessments**'. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and the FOCUS Risk Assessment document (updated annually) which shall include all elements of this standard in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS has implemented an integrated control system characterized using different control types (e.g., layered, preventative, detective, corrective, and compensating) that mitigates identified risks.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Risk Assessments

REFERENCED STANDARDS FOR 17 RISK MANAGEMENT

1704.03b1Organizational.12	HITRUST 03.b Performing Risk Assessments
1707.03c1Organizational.12	HITRUST 03.c Risk Mitigation
1706.03b1Organizational.3	HITRUST 03.b Performing Risk Assessments
1713.03c1Organizational.3	HITRUST 03.c Risk Mitigation
1733.03d1Organizational.1	HITRUST 03.d Risk Evaluation
1780.10a1Organizational.1	HITRUST 10.a Security Requirements Analysis and Specification
1781.10a1Organizational.23	HITRUST 10.a Security Requirements Analysis and Specification
1782.10a1Organizational.4	HITRUST 10.a Security Requirements Analysis and Specification
1783.10a1Organizational.56	HITRUST 10.a Security Requirements Analysis and Specification
1784.10a1Organizational.7	HITRUST 10.a Security Requirements Analysis and Specification
1785.10a1Organizational.8	HITRUST 10.a Security Requirements Analysis and Specification
1786.10a1Organizational.9	HITRUST 10.a Security Requirements Analysis and Specification
17126.03c1System.6	HITRUST 03.c Risk Mitigation

18 Physical & Environmental Security

POLICY:
FOCUS shall ensure that visitor and third-party support access is recorded and supervised unless previously approved. *1801.08b1Organizational.124* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers; and that the FOCUS Review Management System Administrative function shall have a **visitor authorization tracking system** with a screenshot on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to physical security to determine if access of visitors is recorded, and records contain: (i) name and organization of the person visiting; (ii) signature of the visitor; (iii) form of identification; (iv) date of access; (v) time of entry and departure; (vi) purpose of visit; and, (vii) name and organization of person visited. All visitors are supervised unless their access has been previously approved. Access by third-party support personnel is granted restricted access to secure areas or covered information processing facilities only when required, authorized and monitored.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— Data Center visitor(s) and Data Center third-party support access is recorded and supervised unless previously approved, by:
- Data Centers being required to document each visitor access, identify the visitor, verify the visitor as being eligible to enter based on FOCUS eligibility list of visitors in advance; and
- Data Centers being required to document each engineer (support) access, identify the engineer, verify the engineer as being eligible to enter based on FOCUS eligibility list of visitors in advance; and
- That at no time is any person (visitor or engineer) to be allowed to enter the data center without the FOCUS CSO or IT Analysts physically accompanying them at all times in the data center; and
- All Data Center visits by any individual (including FOCUS IT Analysts) are to be authorized, in advance, by the CSO; and
- The FOCUS RMS Administration module/IT Inventory system is to keep a log of all requests/identity of individuals/authorization by the CSO (or not) and notes regarding the nature of the visit, confirmation that the visit occurred, how long the visit was for and notes regarding exactly what was or was not completed during the visit.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that areas where sensitive information (e.g., covered information, payment card data) is stored or processed are controlled and restricted to authorized individuals only. *1802.08b1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers; and that the FOCUS Review Management System Administrative function shall have a **visitor authorization tracking system** with a screenshot on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— Areas where sensitive information (e.g., covered information, payment card data) is stored or processed are controlled and restricted to authorized individuals only, by:
  - Data Centers being required to document each visitor access, identify the visitor, verify the visitor as being eligible to enter based on FOCUS eligibility list of visitors in advance; and
  - Data Centers being required to document each engineer (support) access, identify the engineer, verify the engineer as being eligible to enter based on FOCUS eligibility list of visitors in advance; and
  - That at no time is any person (visitor or engineer) be allowed to enter the data center without the FOCUS CSO or IT Analysts physically accompanying them at all times in the data center; and
  - All Data Center visits by any individual (including FOCUS IT Analysts) is to be authorized, in advance, by the CSO; and
  - The FOCUS RMS Administration module/IT Inventory system is to keep a log of all requests/identity of individuals/authorization by the CSO (or not) and notes regarding the nature of the visit, confirmation that the visit occurred, how long the visit was for and notes regarding exactly what was or was not completed during the visit.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; acquisition logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained in accordance with FOCUS's retention policy. *1803.08b1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— Repairs or modifications to the physical components of a facility which are related to security (e.g., hardware, walls, doors and locks) are documented and retained with the Data Center; and
— The Data Center(s) are to provide FOCUS an online portal to acquire data center access and active certifications; and
— The FOCUS IT Analysts are to log in monthly and download data center access and maintenance logs and store them within the FOCUS Administration/IT Inventory system each month.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access and maintenance logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that fire extinguishers and detectors are installed according to applicable laws and regulations. *1814.08d1Organizational.12* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Physical and Environmental Security**'. Evidence of meeting this standard includes the stipulation that fire extinguishers and detectors are installed according to applicable laws and regulations. While FOCUS is a virtual company with no offices, this standard is applicable to the Primary and Secondary Data Centers. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection against environmental threats to determine if appropriate fire extinguishers are located throughout the facility, and are no more than fifty (50) feet away from critical electrical components; and fire detectors (e.g., smoke or heat activated) are installed on and in the ceilings and floors.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— Data Center fire extinguishers and detectors are installed according to applicable laws and regulations; and
— The Data Center(s) are to provide FOCUS an online portal to acquire maintenance logs or active certifications; and
— The FOCUS IT Analysts are to log in monthly and download data center access and maintenance logs and store them within the FOCUS Administration/IT Inventory system each month.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access and maintenance logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Maintenance and service shall be controlled and conducted by authorized personnel in accordance with supplier-recommended intervals, insurance policies and the FOCUS maintenance program, taking into account whether this maintenance is performed by personnel on site or external to FOCUS. *1819.08j1Organizational.23* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the equipment maintenance to determine if equipment is maintained in accordance with the supplier's recommended service intervals and specifications. Only authorized maintenance personnel carry out repairs and service the equipment. Appropriate controls are implemented when equipment is scheduled for maintenance (e.g., authorization levels) taking into account whether this maintenance is performed by personnel on site or external to the organization.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— For FOCUS Owned hardware and software, maintenance and service are controlled and conducted by:
- Authorized personnel (FOCUS IT Analysts) in accordance with supplier-recommended intervals; and
- Insurance policies (maintenance agreements, such as for the Firewall) are maintained on file within the FOCUS Administration module/IT Inventory system; and
- Per FOCUS policy, no third party vendor is to access any FOCUS Hardware or Software within the data center at any time.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access and maintenance logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that electronic and physical media containing covered information is securely sanitized prior to reuse, or if it cannot be sanitized, is destroyed prior to disposal. *1825.08l1Organizational.12456* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Storage and Destruction Policy**'. Evidence of meeting this standard includes the Storage and Destruction v 12.0.pdf document in PDF format; and photographic evidence of the destruction of each media destroyed which is cataloged within the FOCUS Review Management System in the IT Administrative function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the secure disposal or re-use of equipment to determine if disk wiping or degaussing is used to securely remove electronic information. Shredding, disintegration, grinding surfaces, incineration, pulverization, or melting are used to destroy electronic and hard copy media. Devices containing covered information are physically destroyed or the information is destroyed, deleted or overwritten using techniques to make the original information non-retrievable rather than using the standard delete or format function. The organization renders information unusable, unreadable, or indecipherable on system media, both digital and non-digital, prior to disposal or release for reuse using organization-defined sanitization techniques and procedures in accordance with applicable federal and organizational standards and policies. The organization destroys media containing sensitive information that cannot be sanitized.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Electronic and physical media containing covered information is securely sanitized prior to reuse; or
— If it cannot be sanitized, is destroyed prior to disposal.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; storage and destruction logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
FOCUS shall securely dispose of media containing sensitive information. *1826.09p1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a document entitled '**Storage and Destruction v 12.0.pdf**'. Evidence of meeting this standard includes the stipulation that FOCUS securely disposes of media containing sensitive information. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and photographic evidence of the disposal of each media, which is cataloged within the FOCUS Review Management System in the IT Administrative function. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the disposal of media to determine if the organization destroys (e.g., disk wiping, degaussing, shredding, disintegration, grinding, incineration, pulverization or melting) media when it is no longer needed for business or legal reasons.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS securely disposes of media containing sensitive information.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; storage and destruction logs.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
FOCUS shall develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides; issues authorization credentials for facility access; reviews the access list and authorization credentials periodically but no less than quarterly; and removes individuals from the facility access list when access is no longer required. *1844.08b1Organizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and that the FOCUS Review Management System Administrative function shall have a **visitor authorization tracking system** with a screenshot on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a monthly basis, these FOCUS policies and cross reference the FOCUS inventory of authorized personnel with that on file at the data center(s); and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— FOCUS develops, approves and maintains a list of individuals with authorized access to the facility where the information system resides by:
  • Maintaining an authorized personnel inventory in the FOCUS Administration module/IT Inventory system; and
  • Cross-referencing this inventory on a monthly basis with data on file at each data center; and
— Issues authorization credentials for facility access by:
  • The FOCUS IT Analysts enter requestors into the FOCUS Administration module/IT Inventory tracking system for approval (or disapproval) by the CSO; and
— The FOCUS CSO reviews the access lists and authorization credentials monthly; and
— The FOCUS CSO removes individuals from the facility access list when access is no longer required.

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Quarterly review to ensure compliance.

EVIDENCE:
• Meeting minutes; policy approvals; data center access and maintenance logs.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
For facilities where the information system resides, FOCUS shall enforce physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that FOCUS determines necessary for areas officially designated as publicly accessible. *1845.08b1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. While FOCUS is a virtual company with no offices, this standard is applicable to the Primary and Secondary Data Centers. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and that the FOCUS Review Management System Administrative function shall have a **visitor authorization tracking system** with a screenshot on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensure that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— For facilities where the information system resides (data centers), FOCUS enforces physical access authorizations at defined entry/exit points to the facility where the information system resides, maintains physical access audit logs, and provides security safeguards that FOCUS determines necessary for areas officially designated as publicly accessible by:
  - The requirement that Data Center(s) are to provide FOCUS an online portal to acquire data center access and active certifications; and
  - The FOCUS IT Analysts is to log in monthly and download data center access and maintenance logs and store them within the FOCUS Administration/IT Inventory system each month.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access and maintenance logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required. *18127.08l1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. This FOCUS policy is found in a section entitled '**Surplus Equipment**'. Evidence of meeting this standard includes the stipulation that surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Surplus equipment is stored securely while not in use, and disposed of or sanitized when no longer required by:
- Instructing the FOCUS IT Analysts to evaluate equipment utilization and re-purposing or deprecation quarterly; and
- Upon identifying equipment that is scheduled for re-purposing or deprecation, entries are to be made into the FOCUS RMS Administration module/IT Inventory system; and
- Any equipment with storage device(s) (e.g., hard disk drives) are to be sanitized thoroughly before being re-purposed or removed from equipment and physically destroyed, per the FOCUS Storage and Destruction policy; and
- All equipment not contained within the data center is to be sanitized immediately upon removal from the data center and stored securely until re-purposed or destroyed entirely.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS Storage and Destruction policy; FOCUS RMS Administration module/IT Inventory system reports.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
FOCUS shall ensure the risk of information leakage to unauthorized persons during secure media disposal is minimized. If collection and disposal services offered by other organizations are used, care is taken in selecting a suitable contractor with adequate controls and experience. *18130.09p1Organizational.24* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is the policy of FOCUS that use of third party disposal service firms is strictly prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS ensures the risk of information leakage to unauthorized persons is mitigated through the use of our own FOCUS IT Analysts following the FOCUS Storage and Destruction policy.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS Storage and Destruction policy; FOCUS RMS Administration module/IT Inventory system reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
Disposal methods shall be commensurate with the sensitivity of the information contained on the media. *18131.09p1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the disposal of media to determine if procedures for the secure disposal of media containing information is commensurate with the sensitivity of that information.
The following items are addressed:
i. the use of generally accepted, secure disposal or erasure methods (see 08.l) for use by another application within the organization, for media that contains (or might contain) covered information; and
ii. the identification of information that qualifies as covered. Otherwise a policy is developed that all information is considered covered in the absence of unequivocal evidence to the contrary.

NOTE: It is the policy of FOCUS that use of third party disposal service firms is strictly prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Disposal methods are commensurate with the sensitivity of the information contained on the media by:
• All FOCUS media (e.g., hard disk drives) regardless of data type or kind (including covered data) are to be physically destroyed per the FOCUS Storage and Destruction policy.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS Storage and Destruction policy; FOCUS RMS Administration module/IT Inventory system reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
Fire authorities shall be automatically notified when a fire alarm is activated. *1862.08d3Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Fire authorities are automatically notified when a fire alarm is activated by:
- Service Level Agreement commitments which provide evidence by the data center(s) that mechanisms are in place to provide automated notifications in the event of a fire; and
- Data Centers are to provide FOCUS with a portal for FOCUS IT Analysts to log in and download reports, certifications and testing of the fire alarm systems to be stored within the FOCUS Administration module/IT Inventory system.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS RMS Administration module/IT Inventory system reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
FOCUS shall formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e.g., through policy, standards, guidelines, and procedures). *1863.08d1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. While FOCUS is a virtual company with no offices, this standard is applicable to the Primary and Secondary Data Centers. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e.g., through policy, standards, guidelines, and procedures) by:
  - Service Level Agreement commitments which provide evidence by the data center(s) that mechanisms are in place to provide purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program; and
  - Data Centers are to provide FOCUS with a portal for FOCUS IT Analysts to log in and download data center policies, reports and certifications to be stored within the FOCUS Administration module/IT Inventory system.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS RMS Administration module/IT Inventory system reports.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Storage and Destruction Policy

POLICY:
FOCUS shall ensure that access to network equipment is physically protected. *1892.01|1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. While FOCUS is a virtual company with no offices, this standard is applicable to the Primary and Secondary Data Centers. Evidence shall be on file of the FOCUS Security Policy and Procedure document in PDF format; and the requirement integrated into Agreements with Data Center service providers. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e.g., through policy, standards, guidelines, and procedures) by:
  • Service Level Agreement commitments which provide evidence by the data center(s) that mechanisms are in place to provide purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program; and
  • Data Centers are to provide FOCUS with a portal for FOCUS IT Analysts to log in and download data center policies, reports and certifications to be stored within the FOCUS Administration module/IT Inventory system; and
  • Access to network equipment is physically protected within the data centers (e.g., locked cabinets).

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Quarterly review to ensure compliance; and
• Photography of secured, locked cabinet(s).

EVIDENCE:
• Meeting minutes; policy approvals; photography of secured, locked cabinets.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its equipment maintenance program (e.g., through policy, standards, guidelines, and procedures). *18108.08j1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the equipment maintenance to determine if a formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS formally addresses the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities and compliance requirements for its physical and environmental protection program (e.g., through policy, standards, guidelines, and procedures) by:
- PURPOSE: To ensure that FOCUS equipment (hardware/software) is vetted and tested to uphold all aspects of security, operability, reliability, ease of use and functioning required to facility FOCUS offered services, on the short term/mid term/long term; and
- SCOPE: To ensure that FOCUS equipment is researched, tested and proven secure and beneficial, successfully deployed in testing and production environments, and is able to be maintained when needed, and properly re-purposed and ultimately destroyed when appropriate; and
- ROLES: To ensure that FOCUS stakeholders (FOCUS Employees, contracted peer reviewers and client-companies) have a venue to report successes or failures of all FOCUS equipment so that FOCUS can reach the goal of 100% optimized, operational functionality; and
- RESPONSIBILITIES: To ensure that FOCUS CSO and IT Analysts are engaged in the companywide objective of maintaining fully functioning equipment to facilitate FOCUS services provided to client-companies, all while maintaining superlative security mandates; and
- MANAGEMENT COMMITMENT: To ensure that the FOCUS Administrative team is in full agreement to support all FOCUS Information Technology initiatives to ensure security, functionality and operational 'uptime', including financial support and personnel to achieve this goal; and
- COORDINATION: To ensure that the FOCUS Administration team holds pre-determined (scheduled) as well as ad-hoc meetings to monitor security and performance quality, with business information to prepare for future needs; and coordination between the FOCUS CSO and FOCUS IT Analysts to manage day-to-day operations and mid-term/long-term objectives for the company while upholding all FOCUS policies and procedures; and
- COMPLIANCE: To ensure that FOCUS continues the monthly compliance research by the CSO, and implements or modifies FOCUS policies, procedures and processes to fulfill all compliance (legal, regulatory, accreditation and certification) requirements.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall maintain a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations. *18109.08j1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management.. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; and that the FOCUS Review Management System Administrative function shall have a **visitor authorization tracking system** with a screenshot on file. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the equipment maintenance to determine if the organization: (i) establishes a process for maintenance personnel authorization and maintains a list of authorized maintenance organizations or personnel; (ii) ensures that non-escorted personnel performing maintenance on the information system have required access authorizations; and, (iii) designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— FOCUS maintains a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations by:
  - The requirement that Data Center(s) are to provide FOCUS an online portal to acquire data center authorized personnel for FOCUS systems access; and
  - The FOCUS IT Analysts are to log in monthly and download data center access logs and store them within the FOCUS Administration/IT Inventory system each month; and
  - To reiterate, FOCUS prohibits any individual other than authorized FOCUS employees listed within the FOCUS Administration module/IT Inventory for authorized data center personnel, which is limited to FOCUS Employees, from accessing FOCUS systems.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall monitor and control nonlocal maintenance and diagnostic activities; and prohibits nonlocal system maintenance unless explicitly authorized, in writing, by the CSO or his/her designated representative. *18110.08j1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that access or modifications to any FOCUS owned hardware by third party individual or company is strictly prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS is a virtual company, with no traditional 'offices' to manage access for, except data center(s); therefore
— (HITRUST Standard): FOCUS maintains a list of authorized maintenance organizations or personnel, ensures that non-escorted personnel performing maintenance on the information system have required access authorizations, and designates organizational personnel with required access authorizations and technical competence to supervise the maintenance activities of personnel who do not possess the required access authorizations by:
    - It is FOCUS policy that access or modifications to any FOCUS owned hardware by third party individual or company is strictly prohibited, therefore only FOCUS CSO or IT Analysts are provided access to FOCUS hardware, regardless if it is employee workstation system (utilized in their at-home office) or within the FOCUS datacenter.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; data center access logs.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall obtains maintenance support and/or spare parts for defined key information system components (defined in the applicable security plan) within the applicable Recovery Time Objective (RTO) specified in the contingency plan. *18111.08j1Organizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS obtains maintenance support and/or genuine spare parts solely from the original manufacturer of the equipment; and
— When possible, prior to deployment in production environment, test the repaired/updated equipment in the test environment; and
— All technical support (telephonic) must be acquired directly from the original manufacturer of the equipment; and
— For systems designated as critical, the IT Analyst must prioritize service or repairs in an effort to meet or exceed the defined Recovery Time Objectives (RTO) within FOCUS policies and documentation for that service.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Quarterly review to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; applicable policies for RTO.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

REFERENCED STANDARDS FOR 18 PHYSICAL AND ENVIRONMENTAL SECURITY

1801.08b1Organizational.124	HITRUST 08.b Physical Entry Controls
1802.08b1Organizational.3	HITRUST 08.b Physical Entry Controls
1803.08b1Organizational.5	HITRUST 08.b Physical Entry Controls
1814.08d1Organizational.12	HITRUST 08.d Protecting Against External and Environmental Threats
1819.08j1Organizational.23	HITRUST 08.j Equipment Maintenance
1825.08l1Organizational.12456	HITRUST 08.l Secure Disposal or Re-Use of Equipment
1826.09p1Organizational.1	HITRUST 09.p Disposal of Media
1844.08b1Organizational.6	HITRUST 08.b Physical Entry Controls
1845.08b1Organizational.7	HITRUST 08.b Physical Entry Controls
18127.08l1Organizational.3	HITRUST 08.l Secure Disposal or Re-Use of Equipment
18130.09p1Organizational.24	HITRUST 09.p Disposal of Media
18131.09p1Organizational.3	HITRUST 09.p Disposal of Media
1862.08d1Organizational.3	HITRUST 08.d Protecting Against External and Environmental Threats
1863.08d1Organizational.4	HITRUST 08.d Protecting Against External and Environmental Threats
18108.08j1Organizational.1	HITRUST 08.j Equipment Maintenance
18109.08j1Organizational.4	HITRUST 08.j Equipment Maintenance
18110.08j1Organizational.5	HITRUST 08.j Equipment Maintenance
18111.08j1Organizational.6	HITRUST 08.j Equipment Maintenance

19 Data Protection & Privacy

Data Classification

All FH data is considered company-classified material. This means that all data is covered by our security policy and nothing is allowed to be stored locally, printed or distributed to any company or person *except* to other FH staff members, peer reviewers or client-companies. Printing is prohibited, as the FOCUS Review Management System is a fully automated information management platform. Further, FOCUS has worked to segregate all client-company data in a manner to prevent exposure of one client-companies' records to any other client-company. To this end, all communications (email, phone conversations, etc.) must be scrutinized and staff members or peer reviewers must ensure that information sent to our client-company managers or care managers is solely concerning members of their company.

PHI availability to Third Parties

FOCUS shall make available any and all information requested by applicable Federal or State law, Court Orders or subpoenas. FOCUS will notify the applicable client-company(s) within 24 hours of receipt of Court Order subpoenas.

POLICY:
FOCUS shall implement written policies and/or documented procedures to protect the confidentiality of *individually-identifiable health information* that:URAC C16 (No Weight)

(a) Identifies how *individually-identifiable health information* will be used; (Mandatory)
(b) Specifies that *individually-identifiable health information* is used only for purposes *necessary for conducting the business of FOCUS, including evaluation activities;* (Mandatory)
(c) Addresses who will have access to individually-identifiable health information collected by FOCUS; (Mandatory)
(d) Addresses oral, written or *electronic* communication and records that are transmitted or stored; (Mandatory)
(e) Address the responsibility of *organization* employees, committee members and board members to preserve the confidentiality of *individually-identifiable health information*; **and** (Mandatory)
(f) Requires employees, committee members and board members of FOCUS to sign a statement that they understand their responsibility to preserve confidentiality. (Mandatory)

These URAC standards are implemented within the **FOCUS Security Policy and Procedure**(a)(b)(c)(d)(e)(f). Measurement of success is based on the creation, maintenance, and accurate execution of FOCUS Policies and procedures that meet or exceed each of the above standards; and additional evidence as documented in committee meetings. Ongoing quality assurance monitoring mechanisms include annual review of the programs, policies and procedures, and ongoing monitoring of reports and logs with quarterly committee meetings. All annual and monitoring activities are to be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly committee meetings to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED POLICY:
- Confidentiality of Personal Health Information (PHI)

POLICY:
FOCUS shall formally appointed a qualified data protection officer, reporting to senior management, and who is directly and fully responsible for the privacy of covered information. *1901.06d1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format; the j**ob description** of the Chief Security Officer (Which currently includes the title of Chief Security Officer); and the **FOCUS organizational chart.** Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection and privacy of covered information to determine if there is an appointment of a person responsible, such as a data protection officer or privacy officer, who reports directly to the highest level of management in the organization (e.g., a CEO), and is responsible for the organization's individual privacy protection program, and such appointment is based professional qualities and, in particular, expert knowledge of data protection law and practices and the ability to fulfill required tasks.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Based on annual documented meetings within the FOCUS Administrative Team (composed of the CEO/CMO/CSO/COO/CFO), the formal appointment of a qualified data protection officer, reporting to senior management, and who is directly and fully responsible for the privacy of covered information is to be appointed; and
— In the event for any reason, the appointed data protection officer is unable to execute his/her responsibilities as the appointed data protection officer, the FOCUS CEO is to be responsible for his/her responsibilities until either:
  • The appointed data protection officer returns; or
  • If the appointed data protection officer is unable (for any reason) to return to duties, the FOCUS Administrative Team shall convene an ad-hoc committee meeting to appoint a new data protection officer.

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Documented quarterly meetings to ensure compliance.

EVIDENCE:
• Meeting minutes; policy approvals; Chief Security Officer Job Description; FOCUS organizational chart.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

REFERENCED SUPPORTING DOCUMENT:
• FOCUS Organizational Chart

POLICY:
When required, consent shall be obtained before any protected information (e.g., about a patient) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to FOCUS. *1902.06d1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. To accommodate policy and procedures to fulfill this policy, FOCUS has created a separate document entitled **'Consumer Communication v12.0.pdf'** for detailed instructions. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure document in PDF format. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that divulging of any covered information to any requestor other than the client-company clinical representative, FOCUS Employee or FOCUS contracted Peer Reviewer are prohibited, except where required by law.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— HITRUST Standard: When required, consent is obtained before any protected information (e.g. about a patient) is emailed, faxed, or communicated by telephone conversation, or otherwise disclosed to parties external to FOCUS; however:
  • Based on FOCUS policy of non-communication above, please refer to the FOCUS policy entitled 'Consumer Communication v12.0.pdf' for explicit instructions of protectionary steps to take under a variety of information inquiries and scenarios.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The confidentiality and integrity of covered information at rest shall be protected using an encryption method appropriate to the medium where it is stored; where FOCUS chooses not to encrypt covered information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO. *1903.06d1Organizational.3456711* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure; and **screenshots** of encryption settings for the Mac OSX FileVault whole disk encryption; and details in the policy regarding the encryption algorithm and bit depth. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection and privacy of covered information to determine if covered information, at minimum, is rendered unusable, unreadable, or indecipherable anywhere it is stored, including on personal computers (laptops, desktops) portable digital media, backup media, servers, databases, or in logs; exceptions are authorized by management and documented. Encryption is implemented via one-way hashes, truncation, or strong cryptography and key-management procedures. Acceptable encryption algorithms and strengths are AES-CBC or Triple DES with a 128-bit key minimum (256-bit key for cloud services). For full-disk encryption, logical access is independent of O/S access and decryption keys not tied to user accounts. The information system protects the confidentiality and integrity of information at rest. If encryption is not applied because it is determined to not be reasonable or appropriate, the organization documents its rationale for its decision or uses alternative compensating controls other than encryption if the method is approved and reviewed annually by the CISO.

NOTE: It is FOCUS policy that encryption of covered information is required in all forms (transport, storage, or backups).

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— HITRUST Standard: The confidentiality and integrity of covered information at rest is protected using an encryption method appropriate to the medium where it is stored; where FOCUS chooses not to encrypt covered information, a documented rationale for not doing so is maintained or alternative compensating controls are used if the method is approved and reviewed annually by the CISO; therefore:
  - The HITRUST standard requiring explanations for un-encrypted covered information is not applicable as there is no covered information not encrypted at any time; and
  - MacOS FileVault encryption software utilizes XTS-AES-128 encryption with a 256-bit key; and
  - The FileMaker Server (DBMS Tool deployed by FOCUS which serves the RMS) utilizes the two-way AES-256 encryption that uses a composite key based on information from the machine to encrypt the password and stores the password securely on the server.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots of FileVault MacOS whole-disk encryption.

RESPONSIBLE PARTY:
- FOCUS IT Analyst

POLICY:
FOCUS shall ensure that records with sensitive personal information are protected during transfer to organizations lawfully collecting such information. *1911.06d1Organizational.13* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the stipulation that records with sensitive personal information are protected during transfer to organizations lawfully collecting such information; and **screenshots** of encryption settings for the FOCUS web portal indicating Secure Socket Layer (SSL) 2,048 bit certificate status; and a **screenshot** of the FOCUS Review Management System security configuration settings, and only from/to entities listed within the policy. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

FOCUS shall examine policies and/or standards related to the protection and privacy of covered information to determine if organizations explicitly identify and ensure the implementation of security and privacy protections for the transfer of organizational records, or extracts of such records, containing sensitive personal information to a state or federal agency or other regulatory body that lawfully collects such information.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Records with sensitive personal information are protected during transfer to organizations lawfully collecting such information only under the following circumstances:
- Transmitting protected information, as required, to an active/credentialed contracted Peer Reviewer to conduct the requested request (review) by the FOCUS client-company; and
- Transmitting protected information, as directed, to the client-company per instructions (within the Master Services Agreement (MSA) and any addendums to the MSA) that initiated the review (request) that was conducted; and
- Transmitting protected information upon receipt of a legitimate, verified law enforcement or United States federal entity subpoena.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots of SSL encryption utilized during transport.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensure that covered information storage is kept to a minimum. *19242.06d1Organizational.14* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the stipulation that covered information storage is kept to a minimum; and a **screenshot** of Federal, State and Contractural requirements regarding data retention that result in final stipulations within the FOCUS Policy. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— HITRUST Standard: Covered information storage is kept to a minimum; however:

- It is the policy of FH to retain all data indefinitely, or until a storage limitation is reached. Technology today affords the ability for FH to retain data for years to come. FH retains all data for a minimum of 10 years as required by Federal Law. Due to FOCUS strategy in place with the Review Management System (which encapsulates all data acquired, authored and managed by FH and its client-companies), data is confined to a singular, efficient space; and
- Based on FOCUS Administration decisions, FOCUS is to securely retain data indefinitely until a given client-company terminates an agreement (whereby the Agreement dictates how delivery and/or destruction is to take place) (with the exception of the Medicare 10 year data retention rule); or by directive from a current client-company to destroy data (with the exception of the Medicare 10-year retention rule); and
- FH takes all covered information 'offline' that is older than two years. Two years of data is required to be 'online' and accessible by auditors for client-company audit purposes; and
- Per HITRUST control, all data must be retained a minimum of 6 years, unless otherwise required by law or agreement.

MONITORING:
The FOCUS CSO monitors:

- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance.

EVIDENCE:

- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:

- FOCUS Chief Security Officer

POLICY:
FOCUS shall specify where covered information can be stored. *19243.06d1Organizational.15* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the stipulation that FOCUS specifies where covered information can be stored. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

NOTE: It is FOCUS policy that data storage in any method (paper/images/electronically) outside of an authorized, contracted (MSA/BAA) FOCUS data center is strictly prohibited.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— FOCUS specifies where covered information can be stored; and
— The CSO shall instruct FOCUS IT Analysts to only store covered information within the contracted (MSA & BAA) official FOCUS data center(s).

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance.

EVIDENCE:
- Meeting minutes; policy approvals; list of contracted FOCUS data centers.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall ensur PHI is safeguarded for a period of fifty (50) years following the death of the individual. *1905.06cHIPAAOrganizational.6* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Due to services rendered by FOCUS to our client-companies, and the fact that FOCUS does not provide direct care to patients, FOCUS policy regarding this standard is limited to Federal, State and Contractural data retention requirement minimums. Evidence to support this standard includes **screenshots** of Federal, State and Contractural requirements regarding data retention that result in final stipulations within the FOCUS Policy. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures through compliance research conducted monthly. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— HITRUST Standard: FOCUS ensures PHI is safeguarded for a period of fifty (50) years following the death of the individual; however:
— Due to services rendered by FOCUS to our client-companies, and the fact that FOCUS does not provide direct care to patients, FOCUS policy regarding this standard is limited to Federal, State and Contractural data retention requirement minimums.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance and
- Monthly compliance research to continually confirm non-applicability to this HITRUST standard.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall document compliance with the notice requirements by retaining copies of the notices issued by FOCUS for a period of six (6) years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement. *1906.06c1Organizational.2* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Due to services rendered by FOCUS to our client-companies, and the fact that FOCUS does not provide direct care to patients, FOCUS policy regarding this standard is limited to Federal, State and Contractual data retention requirement minimums. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures through compliance research conducted monthly. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— HITRUST Standard: FOCUS documents compliance with the notice requirements by retaining copies of the notices issued by FOCUS for a period of six (6) years and, if applicable, any written acknowledgements of receipt of the notice or documentation of good faith efforts to obtain such written acknowledgement; however:
— Due to services rendered by FOCUS to our client-companies, and the fact that FOCUS does not provide direct care to patients, FOCUS policy regarding this standard is limited to Federal, State and Contractural data retention requirement minimums.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research to continually confirm non-applicability to this HITRUST standard.

EVIDENCE:
- Meeting minutes; policy approvals.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS shall document restrictions in writing and formally maintains such writing, or an electronic copy of such writing, as an organizational record for a period of six (6) years. *1907.06c1Organizational.3* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Policy and Procedure PDF; and **screenshots** of Federal or State requirements; and reports which indicate the transmission dates/times on file meeting the six year standard; and Business Associate Agreements with client-companies and vendors to be kept on file meeting the six year standard. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Any/All notices regarding PHI must be maintained for six (6) years regardless if the client-company maintains an active relationship with FOCUS or not, including (but not limited to):
  • FOCUS policies & Procedures; and
  • Client-company Master Service Agreements (MSAs); and
  • MSA Addendums; and
  • Business Associate Agreements (BAAs); and
— Through monthly compliance research, the CSO documents any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding PHI documentation.

MONITORING:
The FOCUS CSO monitor:
• Annual review of this policy and mechanisms to ensure compliance; and
• Documented quarterly meetings to ensure compliance; and
• Monthly compliance research to continually confirm non-applicability to this HITRUST standard.

EVIDENCE:
• Meeting minutes; policy approvals; MSAs; BAAs; FOCUS Policies & Procedures.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall document and maintain the designated record sets that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six (6) years. *1908.06.c1Organizational.4* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes the FOCUS Security Policy and Procedure PDF; and **screenshots** of notifications as required contractually with FOCUS client-companies; and **screenshots** of Federal or State requirements; and reports which indicate the transmission dates/times on file meeting the six year standard; and Business Associate Agreements with client-companies and vendors to be kept on file meeting the six year standard. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Per FOCUS policy (included within this document), 'The release of any covered information to individuals or entities other than a request from the originating client-company that provided FOCUS the originating request for review or request by authorized US Federal or State entity by subpoena, FOCUS is prohibited from disclosing PHI; and
— FOCUS documents and maintains the designated record sets that are subject to access by individuals and the titles of the persons or office responsible for receiving and processing requests for access by individuals as organizational records for a period of six (6) years by:
  • Providing contact information at FOCUS (namely the CSO) within FOCUS Master Service Agreements to client-companies, with instructions and details as to the required process for requesting covered information; and
  • Responding to and complying with authorized subpoena.
— Through monthly compliance research, the CSO documents any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding PHI documentation.

MONITORING:
The FOCUS CSO monitors:
• Annual review of this policy and mechanisms to ensure compliance; and
• Documented quarterly meetings to ensure compliance; and
• Monthly compliance research.

EVIDENCE:
• Meeting minutes; policy approvals; MSAs; BAAs; FOCUS Policies & Procedures.

RESPONSIBLE PARTY:
• FOCUS Chief Security Officer

POLICY:
FOCUS shall document and maintain accountings of disclosure as organizational records for a period of six (6) years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting. *1909.06.c1Organizational.5* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes **screenshots** of disclosure requirements as specified contractually with FOCUS client-companies; and **screenshots** of Federal or State requirements; and a **screenshot** of the FOCUS Review Management System in the **Sensitive Data Request Function** which collects the date/time of the request, FOCUS Staff Member name, client-company name, client company requesting contact name, and details regarding the request as well as authorization of the CSO regarding when and how to release the data securely. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

Should a contracted client-company agreement be canceled, FOCUS contacts the client-company Medical Director or Senior Management to coordinate the delivery of all data provided to FOCUS during the life of the Agreement. Data is to be securely delivered by FOCUS IT staff to client-company by an agreed upon method. Upon confirmation of delivery of client data, FOCUS is to thoroughly and permanently delete all client-company data files in all locations and from all media types, except for data required to be preserved by federal or state law.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Per FOCUS policy (included within this document), 'The release of any covered information to individuals or entities other than a request from the originating client-company that provided FOCUS the originating request for review or request by authorized US Federal or State entity by subpoena, FOCUS is prohibited from disclosing PHI; and
— FOCUS documents and maintains accountings of disclosure as organizational records for a period of six (6) years, including the information required for disclosure, the written accounting provided to the individual, and the titles of the persons or offices responsible for receiving and processing requests for an accounting. This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved by:
  - Documenting any and every disclosure FOCUS makes, which must be maintained for a period of 6 years; and
  - Disclosures to originating client companies, and more importantly, any disclosures to any other entity (such as US Federal or State subpoena is to be maintained in FOCUS records for a period of six [6] years).
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding record retention and the appropriate release of PHI.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
The public shall have access to information about FOCUS's security and privacy activities and is able to communicate with its senior security official and senior privacy official. 19134.05j1Organizational.5 This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes **screenshots** of disclosure requirements and permissions as specified contractually with FOCUS client-companies; and **screenshots** of Federal or State requirements a **screenshot** of the FOCUS Review Management System in the **Sensitive Data Request Function** which collects the date/time of the request, FOCUS Staff Member name, client-company member name, associated client-company name, and details regarding the request as well as authorization of the CSO regarding any release of security and privacy activities to the client-company member; and a screenshot of the FOCUS public website with an invitation and link to email FOCUS to learn about security and privacy activities or to pose questions. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

Privacy Policy

FH has a strict privacy policy which prohibits redistribution of any data entered into the Review Management System (RMS), unless requested by an existing FH stakeholder (client-company manager, FH staff member or FH peer reviewer). Further exceptions to this would be an authenticated state or federal regulator. Requests for information by any party must be directed to the Chief Security Officer. It is the CSO's responsibility to verify the authenticity of the request, the requestor and to release as little information as is required. To prevent unauthorized access, maintain data accuracy, and ensure the correct use of information, FH has put in place appropriate physical, electronic, and managerial procedures to safeguard and secure the information collected and stored.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Per FOCUS policy (included within this document), 'The release of any covered information to individuals or entities other than a request from the originating client-company that provided FOCUS the originating request for review or request by authorized US Federal or State entity by subpoena, FOCUS is prohibited from disclosing PHI; and
— The public has access to information about FOCUS security and privacy activities and is able to communicate with its senior security official and senior privacy official by:
  - Providing clear communication method, available on the FOCUS website, which includes an invitation to 'email us', which clearly indicates the electronic mail address (a link) to initiate an email inquiry; and
  - This requirement is to be included in the FOCUS Terms of Use and Privacy Policy versions that are posted on the public website; and
  - The FOCUS marketing and communications policy is to include this requirement to ensure compliance.
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding public access to FOCUS' security and privacy activities.
— Should a member of our client-companies view a publicly accessible login page for FH, the following verbiage is displayed: *"If you are a patient and have any questions about your care, please contact your insurance provider."*

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
FOCUS's formal policies and procedures, other critical records and disclosures of individuals' protected health information made shall be retained for a minimum of six (6) years; and, for electronic health records, FOCUS retains records of disclosures to carry out treatment, payment and health care operations for a minimum of three (3) years. *19140.06c1Organizational.1* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes **screenshots** of disclosure requirements and permissions as specified contractually with FOCUS client-companies; and **screenshots** of Federal or State requirements; and a **screenshot** of the FOCUS Review Management System in the **Sensitive Data Request Function** which collects the date/time of the request, FOCUS Staff Member name, client-company name, client company requesting contact name, and details regarding the request as well as authorization of the CSO regarding when and how to release the data securely. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Per FOCUS policy (included within this document), 'The release of any covered information to individuals or entities other than a request from the originating client-company that provided FOCUS the originating request for review or request by authorized US Federal or State entity by subpoena, FOCUS is prohibited from disclosing PHI; and
— FOCUS's formal policies and procedures, other critical records and disclosures of individuals' protected health information made are retained for a minimum of six (6) years; and, for electronic health records, FOCUS retains records of disclosures to carry out treatment, payment and health care operations for a minimum of three (3) years by:
  • Documenting any and every disclosure FOCUS makes, which must be maintained for a period of 6 years; and
  • FOCUS does not possess an 'electronic medical record' (EMR) nor an 'electronic health record' (EHR), therefore this portion of the HITRUST standard is not applicable to FOCUS.
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding record retention and the appropriate release of PHI.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Important records, such as contracts, personnel records, financial information, patient records, etc., of FOCUS shall be protected from loss, destruction and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, locked facilities or containers, etc. *19141.06c1Organizational.7* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes **screenshots** of transfer encryption; **screenshots** of whole disk encryption; **screenshots** of perpetual password protection of all data at all times; **screenshots** of duplication of data (backup); and **screenshots** of audit trails of data modification. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Per FOCUS policy (included within this document), 'The release of any covered information to individuals or entities other than a request from the originating client-company that provided FOCUS the originating request for review or request by authorized US Federal or State entity by subpoena, FOCUS is prohibited from disclosing PHI; and
— Important records, such as contracts, personnel records, financial information, patient records, etc., of FOCUS are protected from loss, destruction and falsification through the implementation of security controls such as access controls, encryption, backups, electronic signatures, locked facilities or containers
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding secure storage requirements.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Guidelines shall be issued by FOCUS on the ownership, classification, retention, storage, handling and disposal of all records and information. *19142.06c1Organizational.8* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes retention/protection of data **by policy** that no 3rd party companies are involved in data; and the **job description** of the FOCUS CSO specifying responsibility for handling, storage, protection & disposal of data. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Guidelines are issued by FOCUS on the ownership, classification, retention, storage, handling and disposal of all records and information.
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding secure storage requirements.
— See Data Classification Matrix Below:

Data Type	Classification	Retention
Client-Company Sensitive Information (PHI/PII) for Peer Reviews	Review Data	Online 2 years; Offline (archived) Indefinitely until contract termination or federal law (whichever is longest)
All Personnel Files (including background checks, attestations, etc.)	Personnel Data	Perpetual
Client and Vendor Contracts	Contracts	Perpetual
All other data (policies/procedures; meeting minutes, etc.)	Miscellaneous Data	Perpetual

— See Disposal Instructions Below:
Upon cancellation of contract with a client-company or any other data as ordered by the FOCUS Chief Security Officer, sensitive information (PHI/PII) is either disposed of or returned to the originating client-company per their direction contractually, and disposed from FOCUS systems. Steps to delete 'Review Data' include 1) erasure of the encrypted FileMaker database housing the client company data; and 2) deletion of encrypted binary files that the client-company uploaded to the FileMaker server. If disposal is ordered of FOCUS 'Personnel Data', 'Contracts', or 'Miscellaneous Data', the records with the applilcable FBH FileMaker File table(s) are to be deleted from within the FileMaker database. Upon any category of disposal order by the FOCUS CSO, all backup data is to be deleted from the backup drive as well. Upon deletion, the FOCUS CSO is to personally verify deletion and a document with attestation by the FOCUS CSO is to be created and kept on file with details as to what data was deleted and when.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; screenshots.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

POLICY:
Designated senior management within FOCUS shall review and approve the security categorizations and associated guidelines. *19143.06c1Organizational.9* This requirement is stipulated in the **FOCUS Security Policy and Procedure,** which is reviewed and approved annually by FOCUS management. Evidence of meeting this standard includes **policy** stipulating that FOCUS reviews all policies and procedures at least annually with approval by FOCUS management; and policy stipulating that the **FOCUS Organization Chart** must be reviewed and updated annually by FOCUS management; and a PDF of the FOCUS Organizational Chart. Ongoing quality assurance includes activities where the FOCUS CSO shall review, on a quarterly basis, these FOCUS policies; and ensure that any new requirements are considered and integrated into FOCUS policies and procedures. All annual and monitoring activities shall be entered into the FOCUS Calendar.

PROCEDURES:
The FOCUS CSO ensures that:
— This policy is reviewed/modified/ratified no less than annually; and
— Designated senior management within FOCUS reviews and approves the security categorizations and associated guidelines.
— Through monthly compliance research, the CSO is to document any/all applicable US Federal, State, Accreditation or Certification entity requirements regarding secure storage requirements.

MONITORING:
The FOCUS CSO monitors:
- Annual review of this policy and mechanisms to ensure compliance; and
- Documented quarterly meetings to ensure compliance; and
- Monthly compliance research.

EVIDENCE:
- Meeting minutes; policy approvals; FOCUS Organizational Chart.

RESPONSIBLE PARTY:
- FOCUS Chief Security Officer

REFERENCED STANDARDS FOR 19 DATA PROTECTION AND PRIVACY

1901.06d1Organizational.1	HITRUST 06.d Data Protection and Privacy of Covered Information
1902.06d1Organizational.2	HITRUST 06.d Data Protection and Privacy of Covered Information
1903.06d1Organizational.3456711	HITRUST 06.d Data Protection and Privacy of Covered Information
1911.06d1Organizational.13	HITRUST 06.d Data Protection and Privacy of Covered Information
19242.06d1Organizational.14	HITRUST 06.d Data Protection and Privacy of Covered Information
19243.06d1Organizational.15	HITRUST 06.d Data Protection and Privacy of Covered Information
1905.06.cHIPAAOrganizational.6	HITRUST 06.c Protection of Organizational Records
1906.06.c1Organizational.2	HITRUST 06.c Protection of Organizational Records
1907.06.c1Organizational.3	HITRUST 06.c Protection of Organizational Records
1908.06.c1Organizational.4	HITRUST 06.c Protection of Organizational Records
1909.06.c1Organizational.5	HITRUST 06.c Protection of Organizational Records
19134.05j1Organizational.5	HITRUST 05.j Addressing Security When Dealing with Customers
19140.06c1Organizational.1	HITRUST 06.c Protection of Organizational Records
19141.06c1Organizational.7	HITRUST 06.c Protection of Organizational Records
19142.06c1Organizational.8	HITRUST 06.c Protection of Organizational Records
19143.06c1Organizational.9	HITRUST 06.c Protection of Organizational Records

SAMPLE CONFIDENTIALITY AGREEMENT FOR FH EMPLOYEES:

CONFIDENTIALITY, NON-DISCLOSURE, NON-SOLICITATION, NON-CIRCUMVENTION AND NON-COMPETITION AGREEMENT

This Confidentiality, Nondisclosure, Non-Solicitation, Non-Circumvention and Non-Competition Agreement ("***Agreement***") is entered into this ____ day of _____, 20___, by and between **Focus Health, Inc.**, a Florida limited liability company ("***Company***") and _____ ("***Receiving Party***").

The Parties hereby agree as follows:

1. **Background, Scope and Purpose.** The Company desires to engage the Receiving Party as either an employee or independent contractor to provide professional and/or other services to the Company. Receiving Party acknowledges and agrees that during the course of its, his, or her engagement by, or association with, the Company, Receiving Party will have access to the Company's Confidential Information. Receiving Party acknowledges that if he has already been providing services and assistance to the Company (or its predecessor in interest), the terms of this Agreement shall apply to all such services and assistance previously provided by Receiving Party. Receiving Party further acknowledges and agrees that it is essential to the conduct of the Company's business, the sale of its products and the provision of its services and to the protection of its shareholders' investments that the foregoing information of the Company be kept confidential and that its professional and business relationships be protected. The Company desires to restrict Receiving Party's ability to use the Confidential Information and relationships in competition with the business of the Company during the term of Receiving Party's association the Company and thereafter. For purposes of this Agreement, "**Confidential Information**" means information concerning trade secrets, proprietary data, or other valuable confidential or business information relating to the business, operations, products and services of the Company, including, without limitation, the following: (a) information identifying or tending to identify any of the existing or prospective clients, customers, suppliers, employees, and independent contractors of the Company; (b) information regarding any intellectual property of the Company, including all patents, trademarks, trade names, service marks, and copyrighted materials, and all recipes, menus, copy, ideas, know-how, designs, methods, scripts, processes, procedures, concepts, inventions, recordings, advertising and promotional materials, and computer programs, software, and source codes, whether or not protected under any law; and (c) information pertaining to the customers, prospects, products, services, suppliers, vendors, plans, methods, processes, procedures, techniques, financial statements, and financial forecasts and projections of the Company, and legal and accounting information pertaining to the Company, but excluding any disclosure required by law, by a court of competent jurisdiction, or to respond in good faith to a valid inquiry by a governmental authority and excluding any information that is generally publicly available with respect to the business of the Company or that was known to Receiving Party before he became affiliated with the Company. "Confidential Information" also includes patient/member information, hereinafter referred to as "***Protected Health Information***" or "***PHI***", employee/consultant information, financial information, other information relating to the Company and information proprietary to other companies or persons. The Receiving Party's rights and obligations with respect to Protected Health Information are further described in **Exhibit "A"** attached to this Agreement.

2. **Restrictive Covenants.**

(a) ***Absence of Other Restrictions on Competition***. Receiving Party represents and warrants to the Company that Receiving Party is not a party to any restrictive covenant limiting its, his, or her right to work or perform services for the Company in any capacity whatsoever. Receiving Party shall indemnify and hold harmless the Company from all costs, damages, and liabilities that the Company incurs in connection with any suit or claim arising out of any restrictive contract, covenant, or agreement to which Receiving Party is subject on the date of this Agreement or was subject at the date Receiving Party began employment or its association or engagement with the Company.

(b) ***Restrictive Covenants***. Receiving Party shall not do any of the following, directly or indirectly, in any capacity, either for Receiving Party or on behalf of any other person:

(1) After termination of its, his or her association, employment, or engagement for any reason whatsoever, Receiving Party shall not retain or remove, without the Company's advance written consent, any list, data, book, record, design, manual, drawing, formula, document, schedule, source code, specification,

computer program or software, or other written or electronic information pertaining to the business and financial affairs of the Company.

(2) At any time during its, his or her association with or employment or engagement by the Company and following termination thereof for any reason, except to the extent expressly authorized by the Company or in the course of performing its, his or her duties to the Company, Receiving Party shall not reveal, divulge, or disclose, for any reason or in any manner, to any person who is not an officer, director, or authorized employee, agent or shareholder of the Company any Confidential Information.

(3) Receiving Party understands that the Company may receive from third parties confidential or proprietary information ("**Third-Party Information**") subject to a duty on the Company's part to maintain the confidentiality of such information and to use it only for certain limited purposes. Therefore, during the period that Receiving Party is associated with or employed or engaged by the Company and following termination for any reason, Receiving Party will hold Third-Party Information in the strictest confidence and will not disclose to anyone (other than personnel of the Company who need to know such information in connection with their work for the Company) or use, except in connection with his work for the Company, Third-Party Information unless expressly authorized by a member of the Board in writing.

(4) During the period that Receiving Party is associated with or employed or engaged by the Company, and for a period of two years after termination of the association, employment, or engagement for any reason, Receiving Party shall not, directly or indirectly, for Receiving Party or on behalf of any other person: (a) solicit or attempt to solicit any agent, supplier, customer, contractor, or other person who has a business relationship with the Company to cease to do business with the Company, reduce the amount of business that it historically has done with the Company, or otherwise adversely alter its business relationship with the Company, or accept or conduct any business with any such person; or (b) engage in any business, acquire an interest in any business, or serve as an agent, lender, member, officer, partner, director, employee, investor, proprietor, consultant, employee, representative, or independent contractor of any business, that competes with the Business of the Company, anywhere in the United States.

(5) During the period that Receiving Party is associated with or employed or engaged by the Company, and for a period of two (2) years after termination of the association, employment, or engagement for any reason, Receiving Party shall not, directly or indirectly, for Receiving Party or on behalf of any other person, hire, offer, induce, recruit, solicit, influence, or attempt to influence, any person who either is an employee or independent contractor of the Company or has been an employee or independent contractor of the Company during the last twelve (12) months Receiving Party was employed by the Company, to terminate his or her employment or relationship with the Company for the purpose of working for Receiving Party or any other person, whether or not a competitor of the Company.

Receiving Party shall instruct all the agents, officers, directors, employees, or representatives of Receiving Party, if any, to maintain the confidentiality of all Proprietary Information. Receiving Party shall use all Proprietary Information solely for the purpose of providing services to the Company. Additionally, Receiving Party shall not duplicate or reproduce any Proprietary Information except as necessary to render and furnish services to the Company. If the Company requests the return of any Proprietary Information, Receiving Party promptly (and in any event within five business days) shall return to the Company all Proprietary Information and all copies and any analyses, synopses, summaries, and reproductions of Proprietary Information, provided that Receiving Party shall be entitled to retain, but not duplicate or distribute, a copy of the business plan developed for the Company before the date of this Agreement. Receiving Party acknowledges that the Company makes no warranty or representation concerning the accuracy or completeness of any Proprietary Information.

(c) ***Receiving Party's Acknowledgment as to Reasonableness of Restrictions***. Receiving Party acknowledges, stipulates, and agrees that the preceding restrictions are reasonable as to geographical area, time, and line of business and are reasonably necessary to protect legitimate business interests of the Company, including trade secrets and professional information, other valuable confidential or business information, substantial relationships with existing or prospective customers, and customer goodwill associated with the Company's trade name, ongoing business, and the geographical area in which the Company conducts its business. To the extent the duration, geographical area, or line of business of any of the preceding restrictions would cause them to be unenforceable in a particular jurisdiction, the restrictions automatically will be reformed for purposes of enforcement in that jurisdiction to a duration, geographical area, or line of business that is valid and enforceable in that jurisdiction. Reformation of a restriction to validate its enforcement in any particular jurisdiction, however, will not affect the enforcement of the restriction as stated in any other jurisdiction in which

it is enforceable as stated. Also, the invalidity of a restriction in any particular jurisdiction will not affect the validity or enforcement of the restriction in another jurisdiction where it is otherwise valid. The duration of every restriction set forth in this section will be extended by any period during which Receiving Party is in breach of its, his, or her obligations.

3. **Inventions and Other Work Product.**

(a) ***Assignment of Inventions***. All right, title, and interest, of every kind whatsoever, in the United States and throughout the world, in any copyrights, trademarks, ideas, designs, discoveries, inventions, improvements, modifications, developments, processes, works of authorship, source code, object code, documentation, formulas, data, techniques, know-how, trade secrets or intellectual property or any interest therein, whether or not patentable or capable of copyright or trademark registration or subject to similar protection), made, created, developed, conceived, discovered or reduced to practice by Receiving Party (either alone or with others) while associated with or employed or engaged by the Company and related directly or directly to the services provided to Company by Receiving Party (collectively referred to herein as "**Inventions**") shall immediately be the sole, exclusive and absolute property of the Company and its assigns, and Receiving Party hereby irrevocably assigns all such right, title and interest in such Inventions and any interest therein to the Company. Without limiting the generality of the foregoing, Receiving Party hereby assigns its, his, or her entire right, title and interest in and to all Inventions to the Company.

(b) ***Disclosure of Inventions***. In order to permit the Company to claim rights to which it may be entitled, Receiving Party agrees to promptly disclose to the Company in writing and in confidence (i) all Inventions, and (ii) all patent, copyright and trademark applications and registrations filed by Receiving Party during or within one year after the termination, of Receiving Party's association, employment or engagement by the Company. Receiving Party also agrees to submit to a reasonable and confidential review process under which the Company may determine such issues as may arise under this Section 3.

(c) ***Maintenance of Records***. Receiving Party agrees to keep and maintain adequate and current written records of all Inventions. The records may be in the form of notes, sketches, drawings, flow charts, electronic data or recordings, laboratory notebooks, and any other format. The records will be available to and remain the sole property of the Company at all times. Receiving Party agrees not to remove such records from the Company's place of business except as expressly permitted by Company policy which may, from time to time, be revised at the sole election of the Company for the purpose of furthering the Company's business. Receiving Party agrees to return all such records (including any copies thereof) to the Company at the time of termination of Receiving Party's association, employment or engagement by the Company.

(d) ***Assistance***. Receiving Party agrees to assist the Company at the Company's expense, in every way, to create, secure, vest in its name, evidence, enforce and defend the Company's rights, title and interest in and to the Inventions and any copyrights, patents, trademarks, mask work rights, moral rights, or other intellectual property rights relating thereto in the United States and throughout the world, including, without limitation, (i) the disclosure to the Company of all pertinent information and data with respect thereto, and (ii) the taking of all actions and the execution of all assignments, applications, specifications, oaths, deeds, assignments, recordations, and all other documents and instruments which the Company deems necessary or appropriate in order for it to apply for, obtain, maintain and transfer its rights, title and interest in and to such Inventions, and any copyrights, patents, mask work rights or other intellectual property rights relating thereto. Receiving Party hereby waives and irrevocably quitclaims to the Company any and all claims, of any nature whatsoever, which Receiving Party now has or hereafter may have for infringement of any Invention and any copyrights, patents, trademarks, mask work rights, moral rights, or other intellectual property rights relating thereto.

4. **Remedies.** Receiving Party stipulates that a breach by it, him, or her of any of the covenants in Section 2 or 3 of this Agreement will diminish the value of the Company and will cause irreparable and continuing injury to the Company for which an adequate legal remedy will not exist. Accordingly, Receiving Party stipulates that, if it, he, or she is alleged to have breached any of the covenants of this Agreement, the Company shall pay any amounts owed to Receiving Party into an escrow account with an independent third party pending final determination of the parties' respective rights by a court of competent jurisdiction and, without limiting or excluding any other available remedy, the Company will be entitled to the following remedies: (a) entry by a court having jurisdiction of an order granting specific performance or injunctive relief; without requirement of a bond or proof of monetary damage or an inadequate remedy at law; (b) the recovery from the Receiving Party of all profit, remuneration, or other consideration that the Receiving Party gains from breaching the covenant and any damages suffered by the Company, to the extent ascertainable; and (c) reimbursement from Receiving Party of all

reasonable costs incurred by the Company in enforcing the covenant or otherwise defending or prosecuting any mediation, arbitration, or litigation arising out of the covenant. The Company may exercise any of the foregoing remedies concurrently, independently, or successively.

5. **Governing Law, Jurisdiction, and Venue**. The laws of the State of Delaware and the federal laws of the United States of America, excluding the laws of those jurisdictions pertaining to resolution of conflicts with laws of other jurisdictions, govern the validity, enforcement, construction, and interpretation of this Agreement. Receiving Party and the Company (a) consent to the personal jurisdiction of the state and federal courts having jurisdiction in Tampa, Florida (b) stipulate that a proper and convenient venue for any legal proceeding arising out of this Agreement is Tampa, Florida, for a state court proceeding, or the federal court having jurisdiction in Tampa, Florida for a federal court proceeding, and (c) waive any defense, whether asserted by motion or pleading, that New York, New York, or the federal court having jurisdiction in Tampa, Florida, is an improper or inconvenient venue.

6. **Assignment; Successors.** Receiving Party shall not assign its, his, or her rights or delegate any of its, his, or her obligations under this Agreement, and any attempted assignment or delegation by Receiving Party will be invalid and ineffective against the Company. The Company may assign its rights under this Agreement (including the restrictive covenants set forth in Section 2, which shall be enforceable by the assignee) without Receiving Party's consent to any assignee or successor in interest of its business, whether pursuant to a sale, merger, or sale or exchange of all or substantially all the assets or outstanding stock of the Company. This Agreement is binding on, and inures to the benefit of, the Company's authorized assignees and successors. Upon assignment of the Company's rights under this Agreement, (a) every reference in this Agreement to the "Company" will include the assignee, and (b) if the assignee expressly assumes in writing or by operation of law all the liabilities of the assignor generally or under this Agreement specifically, the assignor will be released from all its obligations to Receiving Party under this Agreement.

7. **Modification; Waiver; Severability.** A waiver, discharge, amendment, or modification of this Agreement will be valid and effective only if evidenced by a writing that is signed by or on behalf of the party against whom the waiver, discharge, amendment, or modification is sought to be enforced. No delay or course of dealing by a party to this Agreement in exercising any right, power, or remedy under this Agreement will operate as a waiver of any right, power, or remedy of that party, except to the extent expressly manifested in writing by that party. The failure at any time of either party to require performance by the other party of any provision of this Agreement will in no way affect the party's right thereafter to enforce the provision or this Agreement. In addition, the waiver by a party of a breach of any provision of this Agreement will not constitute a waiver of any succeeding breach of the provision or a waiver of the provision itself. Whenever possible, each provision of this Agreement should be construed and interpreted so that it is valid and enforceable under applicable law. If a court determines that a covenant or agreement in this Agreement is unenforceable, that covenant or agreement will be deemed separable from the remaining covenants and agreements in this Agreement and will not affect the validity, interpretation, or effect of the other provisions of this Agreement or the application of that covenant or agreement to other circumstances to which it is enforceable.

8. **Notices.** Every notice, demand, consent, or other communication required or permitted under this Agreement will be valid only if it is in writing (whether or not this Agreement expressly states that it must be in writing) and delivered personally or by commercial courier and addressed to the addresses for the parties listed below. A validly given notice, demand, consent, or other communication will be effective on the earlier of its receipt.

9. **Execution; Complete Agreement.** The parties may execute this Agreement in counterparts. Each executed counterpart of this Agreement will constitute an original document, and all of them, together, will constitute the same agreement. Delivery of an executed counterpart of a signature page to this Agreement by facsimile or other electronic means shall be as effective as delivery of a manually executed counterpart of this Agreement. This Agreement will become effective, as of its stated date of execution, when each party has signed and delivered a counterpart of it to the other party. This Agreement records the final, complete, and exclusive understanding of the parties with respect to the matters addressed in it and supersedes any prior or contemporaneous agreement, representation, or understanding, oral or written, by either of them.

[*Signatures on following page.*]

[Signature Page to Confidentiality and Non-Disclosure Agreement]

DATED AS OF_____.

COMPANY:

FOCUS HEALTH, INC.

By: _____
Name:_____
Title:_____

Address: _____
_____
_____

EMPLOYEE/CONTRACTOR:

[if Individual]

_____
Name: _____

[if Entity]

_____

By:_____
Print Name:_____
Title:_____

Address: _____
_____

EXHIBIT "A" to Confidentiality and Nondisclosure Agreement

Privacy of Protected Health Information as required by HIPAA

As a Receiving Party, you understand that you will have access to confidential information that may include, but is not limited to, information relating to Protected Health Information ("***PHI***") which can be divided into two categories:

A. "***Medical record information***" is any information, which relates to an individual's physical or mental condition, medical history or medical treatment and which is obtained from a medical professional or health care institution, from the individual or from the individual's spouse, parent or legal guardian.

B. "***Personal information***" is any individually identifiable information gathered in connection with an insurance transaction from which judgments can be made about an individual's character, habits, avocation, finances, occupation, general reputation, credit, health or any other personal characteristics. Personal information includes an individual's name and address.

1. **Permitted Uses and Disclosures:** Receiving Party is permitted or required to use or disclose Protected Health Information (Protected Health Information has the meanings set out in 45 Code of Federal Regulations 164.501) that the Receiving Party creates for or receives from the Company for purposes of carrying out Receiving Party's duties pursuant to the terms of the Receiving Party Agreement.

Receiving Party may disclose such PHI as necessary for Receiving Party's proper management and administration or to carry out Receiving Party's responsibilities only if:

- The disclosure is required by law; or
- Receiving Party obtains reasonable assurance, evidenced by written contract, from any person or organization to which Receiving Party will disclose such PHI that the person or organization will hold such PHI in confidence and use or further disclose it only for the purpose for which Receiving Party disclosed it to the person or organization or as required by law; and
- The party to whom PHI is disclosed agrees to notify Receiving Party (who will in turn promptly notify the Company) of any instance of which the person or organization becomes aware in which the confidentiality of such PHI was breached.

2. **Prohibition of Unauthorized Use or Disclosure.** Receiving Party will neither use nor disclose PHI Receiving Party creates for or receives from the Company or from another Receiving Party of the Company, except as permitted or required by this Exhibit or as required by law or as otherwise permitted in writing by the Company.

3. **Disclosure to Patients.** Receiving Party will promptly upon the Company's request make available to the Company or, at the Company's direction, to the patient (or the Patient's legal or personal representative) for inspection and obtaining copies of any PHI about the patient which Receiving Party created for or received from the Company and that is in Receiving Party's custody or control, so that the Company may meet its access obligations under 45 Code of Federal Regulations 164.5234.

Receiving Party will, upon receipt of notice from the Company, promptly amend or permit the Company access to amend any portion of the PHI which Receiving Party created or received for or from the Company, so that the Company may meet its amendment obligations under 45 Code of Federal Regulations 164.526.

4. **Disclosure Accounting.** So that the Company may meet its disclosure accounting obligations under 45 Code of Federal Regulations 164.528:

Receiving Party will record for each disclosure that Receiving Party makes to the Company or a third party of PHI that Receiving Party creates or receives for or from the Company, (i) the disclosure date, (ii) a brief description of the PHI disclosed, and (iv) a brief statement of purpose of the disclosure (items i-iv, collectively, the "disclosure information"). For repetitive disclosures, Receiving Party may provide (v) the disclosure information for the first of these repetitive disclosures, (vi) the frequency, periodicity or number of these repetitive disclosures and (vii) the date of the last of these repetitive disclosures. Receiving Party will make this disclosure information available to the Company promptly upon the Company's request.

Receiving Party need not record disclosure information or otherwise account for disclosures of PHI that the Company in writing permits or requires (i) for the purpose of the Company's treatment activities, payments activities, or healthcare operations, (ii) to the patient who is the subject of the PHI disclosed or to that patient's personal representatives, (iii) to persons involved in that patient's healthcare or payment for healthcare, (iv) for notification for disaster relief purposes, (v) for national security or intelligence purposes, or (v) to law enforcement officials or correctional institutions regarding inmates.

Receiving Party must have available for the Company the aforementioned disclosure information for the 6 years preceding the Company's request for such disclosure information (except that Receiving Party need not have disclosure information for disclosures occurring before January 2, 2017).

Receiving Party will make Receiving Party's internal practices, books, and records, relating to Receiving Party's use and disclosure of the PHI Receiving Party creates or receives for or from the Company, available to the Company and to the U.S. Department of Health and Human Services to determine compliance with 45 Code of Federal Regulations Parts 160-64 or this Exhibit.

5. **Reporting.** Receiving Party will report to the Company any use or disclosure of PHI not permitted by this Exhibit, Receiving Party will make the report to the Company within 24 hours after Receiving Party learns of such non-permitted or violating use or disclosure. Receiving Party's report will at least:

   - Identify the nature of the non-permitted or violating use or disclosure;
   - Identify the PHI used or disclosed;
   - Identify who made the non-permitted or violating use or received the non-permitted or violating disclosure;
   - Identify what corrective action Receiving Party took or will take to prevent further non-permitted or violating use or disclosure; and
   - Provide such other information, including a written report, as the Company may reasonably request.

6. **Right to Terminate for Breach.** The Company may terminate any employment, consulting or other agreements with the Receiving Party if it determines that Receiving Party has breached any provision of this Exhibit.

Upon termination of an employment, consulting or other agreement with the Receiving Party, Receiving Party will return to the Company (or, at the direction of the Company, destroy) all PHI, in whatever form or medium (electronic or otherwise) that Receiving Party created for or received from the Company, including all copies of and any data or compilations derived from and allowing identification of any patient who is a subject of the PHI. Receiving Party will complete such return or destruction as promptly as possible, but not later than 30 days after the effective date of the termination of the any employment, consulting or other agreement.

7. **Continuing Privacy Obligation.** Receiving Party's obligation to protect the privacy of the PHI Receiving Party created for or received from the Company will be continuous and survive termination, cancellation, expiration or other conclusion of Agreement.

8. **Amendment to Agreement.** Upon the effective date of any final regulation or amendment to final regulations promulgated by the U.S. Department of Health and Human Services with respect to PHI, this Exhibit and the Agreement of which it is part will automatically amend such that the obligations they impose on Receiving Party and the Company remain in compliance with these regulations.

9. **Conflicts.** The terms and conditions of this Exhibit will override and control any conflicting term or condition of the Agreement. All non-conflicting terms and conditions of the Agreement shall remain in full force and effect.

- END OF FOCUS SECURITY POLICY AND PROCEDURE -

12134732v2