CONE HEALTH	**Guideline:** ITS Security Configuration Management Procedure	
	Department Responsible: SW-ITS-Administration	**Date Approved:** 02/14/2024
	Effective Date: 02/14/2024	**Next Review Date:** 02/14/2025

INTENDED AUDIENCE:
System administrators

PROCEDURE:
In accordance with the standards set forth under federal and state statutory requirements (hereafter referred to as regulatory requirements), Cone Health is committed to ensuring the confidentiality, integrity, and availability of all protected health information (PHI/ePHI), sensitive, and confidential data (hereafter referred to as covered information) it creates, receives, maintains, and/or transmits.

The purpose of this procedure is to define roles, responsibilities, and processes associated with security configuration management (SecCM). This procedure is meant to compliment the Information Technology configuration management program.

Scope and Goals:
The scope of this procedure is to define the processes associated with SecCM. The goals of this procedure are as follows:

- Define baseline secure configuration requirements for all information technology assets (e.g., devices, media, applications, systems, network servers, infrastructure devices, etc.)
- Define requirements for creating, approving, testing, implementing and monitoring information technology asset configurations.

Responsibilities:
Chief Information Security Officer (CISO):
The CISO is responsible for, but not limited to the following activities:

- Revision, implementation, workforce education, interpretation, and enforcement of this procedure.
- Managing the SecCM program.
- Working with the relevant system and application personnel to define and document system and application configuration and integrity control baselines.
    - These requirements must be reviewed and tested for effectiveness whenever there is a major change to the environment or at least every six months/annually (depending on application), and if needed, updated to reflect any new configuration requirements.
- Working with Information and Technology Services on implementing and maintaining configuration management technology.
- Researching any newly discovered vulnerabilities to determine if they could be used to exploit the configuration standards defined in this procedure. If a potential exploit is found, work with the relevant groups within the organization to update the configuration standards and all related systems as soon as possible.

Information and Technology Services (ITS):
ITS is responsible for, but not limited to the following activities:

- Implementing approved security configurations for all information technology assets (desktops, laptops, smartphones, servers, network infrastructure, etc.) they have authority over.
- Manage configuration management technology designed to enforce security configuration requirements (e.g., mobile device management technology, Microsoft Baseline Configuration Analyzer, data loss protection technology, etc.).
- Assist with security impact analyses and configuration monitoring activities as needed.
- Centrally manage all anti-malware and anti-spam technology and ensure that it is regularly updated and CANNOT be disabled by users.

Application/System Owners:
Application/system owners work with the CISO to define and implement SecCM for the applications and/or systems they have authority over.

Application/System Administrators:
Application/system administrators are responsible for, but not limited to, the following activities:

- Implementing, maintaining, and monitoring security configurations for application or system assets they are responsible for.
- Assisting with security impact analyses and configuration monitoring activities as needed.
- Assisting with the process for determining the appropriate baseline configuration.
- Ensuring implementation of approved changes/upgrades is limited to only authorized individuals.

Application/Software Developers:
Application/software developers are responsible for, but not limited to, the following activities:

- Ensuring that security configurations are built into applications.
- Assisting with security impact analyses and configuration monitoring activities as needed.
- Incorporating secure coding into development practices (i.e., OWASP, Agile, CERT Software Engineering Institute (SEI) Secure Coding Standards, etc.).

Security Configuration Management:
Identifying Configurations:
Secure configuration for information technology assets represents the secure state consistent with security best practice, vendor recommendations, regulatory requirements and Cone Health operational requirements and constraints. For a typical information system, the secure baseline may address configuration settings, software loads, patch levels, how the information system is physically or logically arranged, how various security controls are implemented, and documentation.

The following resources will be utilized, in addition to vendor/manufacturer recommended secure configuration standards, to create Cone Health configuration standards for information technology assets:

- Security Configuration Checklists (https://csrc.nist.gov/Projects/United-States-Government-Configuration-Baseline)
- National Vulnerability Database (https://web.nvd.nist.gov/view/ncp/repository)

- Center for Internet Security (CIS) (https://benchmarks.cisecurity.org/downloads/benchmarks/)
- NSA Cybersecurity Advisories and Guidance (https://www.nsa.gov/Press-Room/Cybersecurity-Advisories-Guidance/)
- CERT SEI Secure Coding Practices (http://www.cert.org/secure-coding/)
- Open Web Application Security Project (OWASP) (https://www.owasp.org/index.php/Main_Page)

Testing Configurations:
Security configurations will be fully tested prior to implementation in the production environment. Due to the number of issues that may be encountered when implementing configurations, a test or development environment will be used for testing security configurations. Production environments will not be used for testing, development, or contain any in-development code.

Resolving Issues and Document Deviations:
Functional problems found during security configuration testing will be examined and either resolved or documented as a deviation from, or exception to, the established security configuration standard (see Information Security Exception Management procedure).

Approving Security Configurations:
Security configurations will be approved by the CISO before being allowed into production. Security configurations will be included in system security plans.

A backup and restore point of the production environment will be established before final implementation. If any unforeseen issues should occur during deployment, then a rollback will be performed. An audit log will also be maintained of all updates.

Configuration Changes:
The security officer, system administrators, and system owners will ensure that changes are formally identified, proposed, reviewed (annually at a minimum), analyzed for security impact, tested, and approved prior to implementation. The CISO must approve all updated security configurations.

System/application owners, ITS, and the CISO will maintain a secure repository of current and previous versions of security configurations for disaster recovery and business continuity purposes.

Cone Health will employ an automated tool to assist with managing and enforcing the configuration baselines for the various systems and applications on the network. This tool is required to have the following capabilities:

- Be able to centrally manage, apply, and verify configuration settings for the systems and applications throughout the organization.
- Be able to audit and monitor the systems it is responsible for managing.
- Be able to detect and respond to unauthorized changes and alert the appropriate personnel.
- Be able to enforce access restrictions.

Baseline Security Configuration Requirements:
A security baseline configuration standard defines an approved set of basic security objectives which must be met by any given asset. The following baseline security configuration requirements are the minimum for all information technology assets. Additional security configuration requirements will be included as appropriate:

- Remove, disable, change, or otherwise secure default, anonymous, and unnecessary administrator/service/system accounts.
- To support the enforcement of minimum necessary, all access control mechanisms used for information systems storing, processing, or transmitting covered information are set to "deny-all." Access to these systems must be obtained following the established access request process (see the Information Access Management process)
- Change all default passwords/passcodes and enforce Cone Health all other Identification and Authentication requirements (see Identification and Authentication procedure)
- Ensure that any shared resources (registers, main memory, secondary storage) are released back to the system, are protected from disclosure to other systems/applications/users, and users cannot intentionally or unintentionally access information remnants, including encrypted representations of information, produced by the actions of a prior user or system process acting on behalf of a prior user.
- Disable unnecessary services, ports, privileges, etc.
- Implement encryption for data at rest for all assets that can store covered information.
- Establish audit logging requirements (see Audit Logging and Monitoring procedure).
- For assets that transmit covered information, implement FIPS-validated cryptographic mechanisms (encryption in transit) to prevent unauthorized disclosure of information (https://www.nist.gov/itl/current-fips).
- Implementing centrally managed anti-malware protection that includes the following requirements:
    - Audit logs will be retained for a minimum of 90 days.
    - Scans for malicious code will occur in real time (upon opening, downloading, executing files, checking removable media when inserted, etc.), and full system scans will occur on a schedule.
    - Malicious code that is identified will be blocked and quarantined, with an alert being sent to the appropriate administrator.
    - Automated controls (i.e., browser settings) will be configured to prompt the user to authorize and restrict the use of mobile code (e.g., Java, JavaScript, ActiveX, PDF, postscript, Shockwave movies, RealPlayer, and Flash animations).
    - Ensuring that the tools used are kept up to date with the latest definitions and software version.
- Do not display passwords when being typed in during the authentication process.
- Ensure that data execution prevention (DEP) is implemented (using either hardware or software) to protect system memory against unauthorized code execution.
- Authentication attempts will be limited to 5 failed attempts and enforces a 30-minute delay (i.e., lockout) without administrator assistance.
- Ensure that password policy and password or PIN management on workstations and any authorized mobile device (including BYOD) are protected against modification by end users

- Establish a list of blacklisted programs that is used to prevent any unauthorized or inappropriate program execution on Cone Health's information systems (i.e., workstations, servers, laptops). This list will be reviewed and updated on an annual basis or sooner if necessary.
- Locations or devices that are deemed inappropriate for covered information storage shall be technically configured to prohibit.

In addition to the previously mentioned requirements, asset specific baseline security configurations are as follows:

Media Configuration Requirements:
Media used to store and transport covered information will be encrypted utilizing 256 AES encryption as a minimum.

Device Configuration Requirements:
The following configuration requirements will be mandatory for all user device (e.g., computers, laptops, tablets, smartphones, etc.) assets:

- Implement or ensure that the device is utilizing 256 AES encryption.
- Enable a lockout screen after 15 minutes of inactivity.
- For all mobile devices that can access or store Cone Health data, remote software version/patch validation and the ability to remotely wipe the device must be possible.
- For all mobile phones that can access or store Cone Health data, the use of a PIN number to unlock the screen must be enforced.
- Specific mobile device configuration requirements are as follows:
    - Disable peer-to-peer/ad hoc networking
    - Enable personal firewall (when appropriate and feasible)
    - Block split tunnels on VPNs
    - Block exposure to client ports
    - Allow only one Wi-Fi connection manager to be active at a time
    - Disable local file sharing
    - Restrict the ability to connect to the wireless and wired networks simultaneously
    - Disable Bluetooth by default (will require the user to enable function when needed)
    - Disable wireless hotspot capability by default (will require the user to enable function when needed
- Mobile devices will be configured in a way that prevents the circumvention of built-in security controls (e.g., jailbreaking or rooting).

Application/System and Network Configuration Requirements:
The following security configurations are mandatory for all Cone Health systems, applications, and network devices.

- Store password files separate from application data using an approved hash algorithm and salt.
- Authentication credentials (i.e., userID and password) will be encrypted at time of entry and during any transmissions.
- Restrict passwords from being used in automated log-on processes.
- Disable the ability to "remember password."

- Disable/block any dial-up capabilities on network equipment.
- Enforce the use of secure encrypted connectivity (e.g., SSL, VPN, SSH, IPSEC) for remote access to the network and between the network and third-party systems (i.e., information exchange).
- Restrict user activities associated with administrative/privileged access (e.g., controlling permissions to files, directories, registry keys, and restricting user activities such as modifying system logs or installing applications) to only those users that have an approved need based on their job responsibilities (i.e., minimum necessary).
- For workstations that are publicly positioned, a time-out mechanism (e.g., a screen saver) pauses session screen after two minutes of inactivity. No password prompt required for reauthentication. Examples of publicly positioned workstations are clinical generics (i.e., nursing stations) and workstations in patient rooms.
- Enable a lockout screen after 15 minutes of inactivity.
- After 30 minutes of inactivity network sessions will close (i.e., session timeout) and will require the user to reestablish access.
- Enable session/remote connectivity security settings based on internal policy/procedure (see Information Access Management procedure).
- Applying network protections (e.g., TLS, IPSEC).
- Applying vendor-released patches in response to identified vulnerabilities, including software updates within in a timely manner, and using the latest version of web browsers.
- Anti-spam and anti-malware protection are implemented at information system entry/exit points of the network.
- File integrity monitoring implemented.
- Use of host-based firewalls or port filtering tools.
- Disable unnecessary services and ports.
- Disable unnecessary network protocols and network interfaces.
- When possible, access rights to applications and application functions will be limited to the minimum necessary, using menus (e.g., read, write, delete, and execute).
- Identification and authentication will be required each time a different application or system is accessed (i.e., one system/application will not act as a single means of identification and authentication).
- Outputs from applications handling covered information will be limited to specifically authorized locations (i.e., business machine, printer, terminal, etc.).
- Include a link to or publish in text, the organizational privacy and data use policy on all system connections that allow external parties to access Cone Health's information systems such as web sites, web-based applications, and public access terminals.

Personal Device Configuration Requirements:

Security configuration requirements for personal devices are defined in the Personal Device Use procedure.

Electronic Commerce System Configuration Requirements:

The following security configurations are mandatory for all Cone Health systems, applications, and network devices that handle electronic commerce (e-commerce) transactions:

- The use of strong access control mechanisms that fulfill all the requirements of identification and authentication (as defined in the Identification and Authentication procedure).
- Implement 256 bit or greater, encryption services for all data at rest and in transit (e.g., SSL, TLS, SSH, HTTPS etc.).
- Implement audit and monitoring mechanisms to track the flow of data and to determine and keep track of if transactions contain any covered information.

System Integrity Requirements:
Maintaining system and data integrity is essential to maintaining the confidentiality, integrity, and availability of critical business data. To minimize these threats, the following controls will be implemented:

Input Error Reporting and Handling:
Input processing requires that controls be identified to verify that data is accepted into the system correctly, and that input errors are recognized and corrected.

Input error handling can be processed by:
- Rejecting only transactions with errors
- Rejecting the whole batch of transactions
- Accepting batch in suspense
- Accepting batch and flagging error transactions

Input control techniques include:
- Transaction log
- Reconciliation of data
- Documentation
- Error correction procedures
- Anticipation
- Transmittal log
- Cancellation of source documents

Data Validation Checks:
Data validation checks shall be conducted throughout the data entry process or automatically by technical tools. Methods for identifying input errors and unauthorized modifications will include:
- Sequence Check
- Limit Check
- Range Check
- Validity Check
- Reasonableness Check
- Table Look-ups
- Existence Check
- Key Verification
- Check Digit
- Completeness Check

- Duplicate Check
- Logical Relationship Check

Data File Controls:

Data file controls will ensure that only authorized processing occurs to data at rest. The types of controls that will be used are as follows:

- Before and After Image Reporting
- Maintenance Error Reporting and Handling
- Source Documentation Retention
- Internal and External Labeling
- Version Usage
- Data File Security
- One-For-One Checking
- Prerecorded Input
- Transaction Logs
- File Updating and Maintenance Authorization
- Parity Checking

Processing Controls:

Processing controls ensure that data in a file or database remains complete and accurate until changed as a result of authorized processing or modification routines. The following processing control techniques will be used to address the issues of completeness and accuracy of accumulated data:

- Manual Recalculations
- Editing
- Run-to-Run Totals
- Programmed controls
- Reasonableness Verification of Calculated Amounts
- Limited Checks on Calculated Amounts
- Reconciliation of File Totals
- Exception Reports

Continuous Monitoring:

Continuous monitoring is a process utilized to validate that information assets are adhering to organizational policies, procedures, and the approved security baseline configuration. Continuous monitoring identifies undiscovered/undocumented system components, misconfigurations, vulnerabilities, and unauthorized changes, all of which, if not addressed, can expose Cone Health to unnecessary risk. Due to the laborious nature of this process, whenever possible, automated tools will be used to efficiently identify when an information asset is not consistent with the approved security configurations and when remediation actions are necessary. Automated tools will:

- Centrally manage, apply, and verify configuration settings.
- Respond to unauthorized changes to network and system security-related configuration settings.
- Enforce access restrictions and support auditing of the enforcement actions.

Continuous monitoring is also accomplished through vulnerability management and compliance assessments.

Virtual Machine Image Monitoring:
The integrity of all virtual machine (VM) images must be ensured at all times. The following monitoring requirements must be in place for all VM images:

- Audit and monitoring capabilities to detect any abnormalities or changes to a virtual machine baseline image (file integrity monitoring).
- If a change is detected, an alert that contains what changed must be sent to appropriate ITS personnel to perform an integrity validation check.
- Change information must be made available and/or communicated to appropriate management members within the organization.

Log-On Banners:
All systems and applications will display login banners. These log-on banners will outline the terms and conditions of access. The following banner will be displayed at the point of user log-on:

> *This system is for the use of authorized users only, and all activities on this system monitored and recorded. Anyone using this system consents to monitoring, and if monitoring reveals possible evidence of criminal activity, Cone Health may provide evidence to law enforcement. Inappropriate use of this system by users will result in disciplinary action up to and including termination.*

Documentation Retention:
Records related to security configuration management will be retained for a period of no less than 6 years from the date of the documentation.

Exception Management:
Exceptions to this procedure will be evaluated in accordance with Cone Health's Information Security Exception Management procedure.

Applicability:
All employees, volunteers, trainees, consultants, contractors, and other persons (i.e., workforce) whose conduct, in the performance of work for Cone Health, is under the direct control of Cone Health, whether or not they are compensated by Cone Health.

Compliance:
Workforce members are required to comply with all information security policies/procedures as a condition of employment/contract with Cone Health. Workforce members who fail to abide by requirements outlined in information security policies/procedures are subject to disciplinary action up to and including termination of employment/contract.