VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Configuration Management Policy	**Policy No.** 5.23 **Revision History Date:** Replaces: VHC-POL-CM Current version: 03/01/2020 Replaces: DCF-POL-CM Current version: 11/01/2016
Attachments/Related Documents:	**Version Number:** 1.0
Name/Title of Authorizing Signature: Michael K. Smith, AHS Secretary	**Origination Date:**
☒**Trauma Informed Review**	

Authorizing Signature: **Effective Date:** 12-15-20

POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Configuration Management Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) in compliance with all applicable State and Federal Law, regulations, or policies, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

BACKGROUND:

This policy follows the NIST SP 800-53 Rev.4 framework. The purpose of this policy is to establish change management and configuration change controls for AHS information systems. These controls include the systematic proposal, justification, implementation, testing, review, and disposition of changes to the systems, including system upgrades and modifications. Configuration change control includes changes to baseline configurations for components and configuration items of information systems, changes to

configuration settings for information technology products such as: operating systems, applications, firewalls, routers, and mobile devices, unscheduled/unauthorized changes, and changes to remediate vulnerabilities.

This policy details how AHS complies with Federal information security standards for implementing and maintaining an information Security Configuration Management Policy.

SCOPE:

This policy governs Information Security protocols related to configuration management and implementation of associated standards and procedures.

ROLES AND RESPONSIBILITES:

AHS Secretary – Responsible for making a final review and approval of this policy.
AHS Policy Committee - Responsible for making a final review of this policy.
Chief Information Security Officer – Responsible for reviewing and approving this policy prior to AHS Policy Committee. The CISO will report all compliance-related activities pertaining to this policy to AHS Secretary.
Authorizing Official - responsible for operating an information system authorized pursuant to AHS Policy 5.08 at an acceptable level of risk to agency operations (including mission, functions, image, or reputation), agency assets, or individual's data.
AHS Information Security Director – responsible for:

- creating procedures and standards to meet the requirements established in this policy.
- reporting all matters pertaining to the AHS's compliance with this policy to the CISO and the Authorizing Official; and
- ensuring that this policy is reviewed at least annually and updated when necessary.

PROTOCOLS:

The AHS Information Security Director will establish associated security standards and procedures to meet the following configuration management requirements.

Baseline Configuration

- Baseline configurations of all AHS information systems will be developed, documented, and maintained under official configuration control and any deviations from the baseline will be approved and documented.
- The information system baseline will be reviewed and updated annually or when significant changes or updates occur.
- Previous versions of baseline configurations of the AHS information systems will be retained to support rollback capabilities and for auditing purposes.

Configuration Change Control

- Types of changes to AHS information systems will be determined and documented.
- A formal change control body made up of technology and system owners will be used to review, approve, and track all changes to AHS information systems.

- Any changes to AHS information systems will be tested and validated before implementing the changes on the system and a rollback plan will be documented should the changes be found to have a negative system or security impact.
- Configuration change decisions associated with AHS information systems will be documented.
- A record of changes to AHS information systems will be retained for a minimum of one year.
- Changes to AHS information systems will be audited and reviewed regularly by internal and external parties, as applicable.
- A formal change control body will coordinate and provide oversight for configuration change control activities.

Security Impact Analysis

- Changes to AHS information systems will be analyzed to determine potential security impacts or associated security ramifications (e.g. to security plan or risk assessment) prior to change implementation.
- Changes to AHS information systems will be analyzed in a separate test environment before implementation in an operational environment, looking for security impacts due to flaws, weaknesses, or incompatibility.
- Processing or storing of Personally Identifiable Information (PII) in test environments is prohibited.
- Security functions will be checked after the AHS information system is changed to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome for meeting the system's security requirements.

Access Restrictions for Change

- Only authorized personnel will be able to implement approved configuration changes.
- Automated mechanisms to enforce access restriction to configuration change information and support auditing of the enforcement actions will be employed.
- Privileges to change information system components and system-related information within a production or operational environment will be limited. Privileges will be reviewed at least quarterly.

Configuration Settings

- Mandatory configuration settings for information technology products (e.g. servers, workstations, network components) employed within AHS information systems will be documented using the latest security configuration guidelines.
- Any deviations from established configuration settings will be identified, documented, and approved.
- Changes to the configuration settings will be monitored and controlled.

Least Functionality

- AHS information systems will be configured to provide only essential capabilities to meet the requirements and purpose of the system.
- AHS information systems will be hardened to include prohibiting, disabling, or restricting the use of unused or unnecessary physical and logical functions, ports, protocols and/or services.

- AHS information systems will be reviewed annually to identify unnecessary and/or insecure functions, ports, protocols, or services and disable those deemed insecure.
- AHS information systems will ensure only authorized software program execution where technically feasible.
- The authorized software list will be reviewed and updated annually.

Information System Component Inventory

- Document an inventory of information system components within the authorization boundary of the information system will be developed and documented.
- The inventory of AHS information system components will be updated as an integral part of component installations, removals, and information system updates.
- The network will be scanned to detect changes, and review and update, the asset inventory on a regular basis.
- Unauthorized devices will be removed from the network if discovered.
- The inventory will be reviewed and updated annually.

Configuration Management Plan

A configuration management plan will be developed, documented, and implemented for AHS information systems that:

- Addresses roles, responsibilities, and configuration management process and procedures.
- Establishes a process for identifying configuration items (i.e., hardware, software, firmware, and documentation) throughout the system development life cycle (SDLC) and for managing the configuration of the system.
- Defines the configuration items for the information system and places the configuration items within the configuration management plan.
- Protects the configuration management plan from unauthorized disclosure, dissemination, and modification.
- Describes how to move changes through the change management process, update configuration settings and baselines, maintain information system component inventories, control development, test, and operation environments, and develop, release, and update key system documentation.
- Software Usage Restrictions Software usage will be in accordance with contract agreements and copyright laws.
- The usage of software will be tracked to protect and control licenses from unauthorized copying and distribution. The use of peer-to-peer file sharing technology will be controlled and documented to ensure there is no unauthorized distribution, display, performance, or reproduction of copyrighted material.
- Open source software will be legally licensed, approved, and adhere to a secure configuration baseline checklist from the U.S. Government or industry.

User Installed Software

- Written processes and procedures will be established to govern the installation of software by end users of computing systems.
- Software installation policies will be enforced through procedural, periodic examination, and/or automated methods.

ENFORCEMENT:

The AHS Secretary may initiate reviews, assessments, or other means to ensure that policies, guidelines, or standards are being followed.

AUTHORITIES:

- Health Insurance Portability and Accountability Act (HIPAA) Security Rule: 45 CFR Part 160 and Subparts A and C of Part 164
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.0, November 10, 2015
- IRS Publication 1075 (Rev. 11-2016)
- Social Security Administration (SSA), *Electronic Information Exchange Security Requirements and Procedures For State and Local Agencies Exchanging Electronic Information With The Social Security Administration* based on: Federal Information Security Management Act (FISMA), Public Law (P.L.) 107-347, the Privacy Act of 1974 and SSA's own policies, procedures and directives
- Criminal Justice Information Services (CJIS), Security Policy, Version 5.7, 08/16/2018, CJSD-ITS-DOC-08140-5.7

REFERENCES:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
CM-1 CM-2 CM-2(1) CM-2(3) CM-3 CM-3 (2) CM-4 CM-4 (1) CM-4 (2) CM-5 CM-5 (1) CM-5 (5) CM-6 CM-6(1) CM-7 CM-7(1) CM-7(2) CM-7(4) CM-8 CM-8(1) CM-8(3) CM-8(5) CM-9 CM-10 CM-11	9.3.5			5.7 5.7.1

(Version numbering instructions: Major revisions are reflected in whole numbers, minor or no revisions in tenths.)

Document Version Control			
Version Number	**Version Effective Date**	**Author**	**Description**
1.0		Emily Wivell	Initial Version

APPENDIX:

None.