VERMONT
AGENCY OF HUMAN SERVICES

AHS Policy Title: 5.15 Information Security Maintenance Policy

Policy Information

Revision Date:

02/21/2023

Revision Number:

1.3

Attachments/Related Documents:

none

Effective Date:

06/01/2020

☒ Trauma Informed Review

☒ Racial Equity Review

Authorizing Signature:

Jenney Samuelson,
Agency of Human Services Secretary

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Maintenance 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.

Background:

NIST Special Publication 800-53, Minimum Acceptable Risk Standards for Exchanges (MARS-E), and IRS Publication 1075 requires AHS to perform periodic and timely maintenance on organizational information systems and to provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct information system maintenance.

This policy assures compliance with state and federal laws relating to information security system and information integrity, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

This policy follows the National Institute of Standard and Technology (NIST) SP 800-53 Rev.5 framework. The purpose of this policy is to establish Information Security Maintenance protocols.

The policy details how AHS complies with Federal information security standards for implementing and maintaining an Information Security System Maintenance Policy.

Scope:

This policy governs AHS Information Security Maintenance protocols and associated standards and procedures.

Roles and Responsibilities:

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 and updated (if necessary) at least annually.

Protocols:

General

The AHS Information Security Director will establish standards and procedures to ensure AHS information systems are maintained as defined in this policy.

If any AHS information system cannot be configured to meet the minimum requirements of this policy, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

Controlled Maintenance

All maintenance activities (local or nonlocal) will be approved and monitored by authorized individuals. Maintenance support and/or system components will be obtained within the applicable Recovery Time Objective (RTO) specified in the contingency plan. If information system components need to be taken off-site for maintenance, the applicable business owner will approve the removal. Equipment will be sanitized before being taken off-site. Following maintenance activities, security controls will be verified to ensure they are working as expected.

Maintenance Tools

Maintenance tools will be approved, controls, and monitored. Tools will be inspected for any improper or unauthorized modifications. Maintenance media will be tested for malicious code before use in information systems.

Nonlocal Maintenance

Nonlocal maintenance is prohibited unless it has been explicitly authorized. If nonlocal

maintenance is authorized the following requirements must be met:

- Explicit approval must be given for personnel to perform nonlocal maintenance and nonlocal maintenance activities are monitored.
- Multi-factor authentication is required for nonlocal maintenance.
- Maintenance records are current and include nonlocal maintenance activities.
- Accounts with the privileges to perform nonlocal maintenance are managed through the agency's account management process and follow identification and authentication requirements.
- All nonlocal maintenance activities to AHS information systems are done so using agency issued information systems.

The use of nonlocal maintenance and diagnostic activities will be established in the information system's security plan. Nonlocal maintenance and diagnostic activities will be monitored, audited, and periodically reviewed.

Maintenance Personnel

A process for authorizing and maintaining a list of authorized maintenance personnel will be established. AHS personnel with required access authorizations and technical competence will supervise maintenance activities of maintenance personnel. If maintenance personnel are not supervised, they will have the required access authorizations.

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
- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.2, September 16, 2021
- IRS Publication 1075 (Rev. 11-2021)
- 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 5.9.1, 10/01/2022, CJSD-ITS-DOC-08140-5.9.1

References:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
MA-1				
MA-2	MA-1			
MA-3	MA-2			
MA-3 (1)	MA-3			
MA-3 (2)	MA-4			
MA-3 (3)	MA-5			
MA-4	MA-6			
MA-4 (1)				
MA-4 (2)				
MA-5				
MA-5 (1)				
MA-6				

Document Review and Revision Control

Version	Review Date	Author/Reviewer	Description
1.0	4/27/2020	Emily Wivell	New AHS Policy Replaced VHC and DCF Policies
1.1	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes
1.2	9/8/2022	Emily Wivell	Annual Renewal
1.3	02/21/2023	Emily Wivell	Annual Renewal

Appendix:

None.