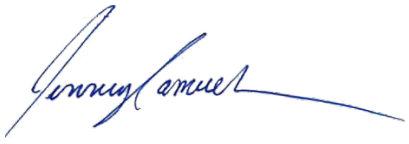
VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: 5.12 Information Security Risk Assessment Policy	**Revision Date:** 7/3/19, 9/1/21, 10/1/22
Attachments/Related Documents:	Revision Number: 1.3
Name/Title of Authorizing Signature: Jenney Samuelson, AHS Secretary	Effective Date: 7/3/19

☒ **Trauma Informed Review**

☒ **Racial Equity Review**

Authorizing Signature: 

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Risk Assessment Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) incompliance with all applicable State and Federal Laws, regulations, or policies.

Background:

HIPAA requires AHS to carry out periodic information security risk assessments to identify "potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information" held by AHS. 45 C.F.R. § 164.308. This Information Security Risk Assessment Policy assures that AHS' risk assessment activities comply with HIPAA requirements through adherence to the standards and guidelines established in NIST 800-53 and 800-30.

Risk assessments are essential components of a holistic risk management process.

Risk assessments identify vulnerabilities in information systems and organizational operations and assess the potential degree of harm and likelihood of harm that could result from the identified risks to allow leadership to prioritize appropriate actions to mitigate the risks.

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 Risk Assessment protocols.

The policy details how AHS complies with Federal information security standards for

implementing and maintaining an Information Security Risk Assessment Policy.

Scope:

This policy governs Information Security Risk Assessments related to the protection of AHS Information Systems and implementation of 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 meet the following risk assessments specifications for the protection of AHS information systems.

If an AHS information system cannot be configured to meet the minimum information security risk assessment standards and procedures, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

Program/components - To support information security responsibilities, AHS has established an Information Security Risk Management (ISRM) program through the adoption of AHS Security Policies. The foundation of this program is NIST SP 800- 30 Rev. 1, Risk Management Guide for Information Technology Systems, whereby regular risk assessments will be performed, and the results of which inform all aspects of AHS's information security program.

Plan for ongoing activities- Effective risk management is not an annual or periodic activity, rather an ongoing process that is integrated in AHS operations. In addition to annual formalized risk assessments, any significant changes to the risk environment or posture will be noted and adjustments to the risk assessment and/or risk register made as needed. To help inform these

ongoing activities, contacts with information security forums and professional associations will be maintained.

Risk Register - AHS has developed and maintains a secure risk register to serve as an inventory of known risks and document AHS's planned remedial actions to correct weaknesses or deficiencies noted as a result of risk management activities to reduce or eliminate known vulnerabilities. This risk register is also updated at least annually based on the findings from security assessments, security impact analyses, and continuous monitoring.

Security Categorization - AHS will define a security categorization for all information systems. All information systems categorized as High or Moderate are considered sensitive or to contain sensitive information. All information systems categorized as Low are considered non-sensitive or to contain non-sensitive information. Security categories will be based -on the potential adverse impacts to organizational operations, assets, and individuals and data.

Availability of information systems - AHS information systems will be evaluated and categorized based on the potential impact to the organization in the event they become unavailable.

Confidential Information - AHS will periodically identify all activities that create, store, and transmit confidential information. This includes the information systems that support these business processes. These processes will be evaluated to determine the level of risk (LOW, MODERATE, or HIGH) associated with each identified activity and associated information system.

Risk Documentation and Reporting - AHS will document the results of risk analysis and will ensure such documentation has been distributed to appropriate members of the workforce responsible for mitigating the threats and vulnerabilities to information systems and to sensitive information.

Risk Management Process

IT Security Risk Management Committee -AHS will establish and maintain an IT Security Risk Management Committee that will function as the governing body to manage the annual risk assessment and decision making related to preventing and mitigating identified IT security risks. The Committee will be facilitated by the Risk Manager and members will include security and business leads from all stakeholder departments.

IT Security Risk Management Committee Meetings - The Risk Management Committee will meet for regularly scheduled meetings in addition to impromptu meetings when potential, high security risks or incidents are brought to their attention. The Risk Manager will schedule and facilitate these meetings.

AHS Security Risk Assessment- Each year the AHS Information Security Team, in conjunction with the IT Security Risk Committee, will assign or hire a third-party

Risk Assessment Team, to conduct, an organization-wide security risk assessment. The report resulting from this risk assessment will include a detailed description of the information security risks currently facing AHS, and specific recommendations for preventing or mitigating these risks.

Risk Assessment Methodology-AHS risk assessments are to be conducted using the guidance in NIST SP 800-30 - Risk Management Guide for Information Technology Systems and encompassing risks related to weakness or absence of expected controls as defined in the appropriate controls framework based on the type of data.

High Information Security Risks - For every high information systems security risk identified – whether through a formal risk assessment or ad hoc discovery-the CISO decides the degree to which AHS will accept the risk or implement mitigating controls to reduce the risk and any expected losses.

Information Systems Risk Management

Information Security Impact Analysis - Whenever sensitive information is to be placed in computers or whenever sensitive information is to be used in new or substantially different ways on computer systems, a risk assessment of the potential security-related impacts will be performed.

System Risk Assessments

Information systems security risk assessments for information systems and applications will be performed at least every two years. All major enhancements, upgrades, conversions, and related changes associated with these systems or applications will be preceded by a risk assessment assigned by the IT Security Risk Management Committee. Specific instances requiring risk assessments include:

1. All systems being implemented or constructed will be assessed for risk during the preliminary design phase.
2. All computer information systems will be reevaluated for risk when they are to be significantly modified or enhanced.
3. All information systems that are being considered for development or deployed by external third parties.

Vulnerability Management

Identification

The detection and identification of vulnerabilities will only be performed by qualified personnel authorized by the CISO. AHS recognizes that there is no "one size fits all" approach to identifying vulnerabilities. Various tools and techniques will be applied to sufficiently and effectively identify the various vulnerability types that may exist. IT and security staff will periodically review the tools and techniques used to determine if changes may result in a more effective identification process. IT and security staff will also receive security alerts, advisories, and directives from credible external organizations on an ongoing basis. Scanning processes will be routinely performed monthly to detect internal and external vulnerabilities.

Outputs from vulnerability assessments will include a prioritized list of findings that include a description of the vulnerability, missing patch, or setting that is misconfigured, and recommended remedies. Scan reports will be reviewed by technical personnel to isolate and remove false positive findings (with documented rationale for removal}, and to prioritize responses to the

remaining vulnerabilities.

Assessment Types

Vulnerability scans can be conducted in a variety of ways. A couple of examples are below:

- **Full:** Full assessments scan the entire environment to generate lists of vulnerabilities such as misconfigured information systems and searching for unknown devices. Depending on the significance of the vulnerability, these assessments may be performed outside of business hours.
- **Targeted:** Targeted scans are performed on specific information systems such as subnets, system types (workstations, firewalls, other network equipment}, and mobile devices.

Penetration testing can also be an effective means to identify vulnerabilities and test controls. Penetration tests will be conducted regularly on external/perimeter systems, as well as periodically on internal systems. Penetration tests will be conducted by qualified external third parties. Because testing services are expensive, testing scopes and approaches can be varied from one test to another to ensure thorough and adequate testing of all attack surfaces over a period of time.

Assessment Tools

Industry standard tools or services will be selected and used to perform internal and external vulnerability scans. Open-source tools may be authorized on a case- by-case basis by the CISO. Vulnerability scanning tools will be updated prior to new scan to be able to scan for new vulnerabilities.

Privileged accounts will be utilized to access scanning tools.

Remediation

Misconfigured Information Systems:

Remediation pertaining to misconfigured systems will be entered into the ticketing system for resolution.

A misconfigured system will be investigated to ensure the system, such as a workstation, is receiving the necessary configuration changes or updates from central management.

System Patching:

Patches will be applied based on criticality after first being implemented in a non- production environment to ensure that patches do not introduce additional vulnerabilities or have a negative operational impact to AHS's production environment. Once the patch has been tested and has been shown not to disrupt information systems on the enterprise network, it will be distributed to production systems.

Metrics:

Metrics will be maintained to gauge and benchmark remediation progress, such as the following:

- Percentage of findings remedied or patched

- Locations of information systems out of compliance
- Time taken to remediate vulnerabilities based on criticality
- The number of findings without or awaiting a remedy
- The number of confirmed false positives

Application Security

Security Assessment:

Security assessments on any new or major releases (e.g., releases that change the version number, 1.XX - to 2.XX), will be performed in a development or test environment to ensure that any new features or upgrades do not interfere with security functionality, other applications and information systems/components in use on the enterprise network.

Vendor assessments will be performed on third party application developers to ensure secure coding practices are used. For applications handling sensitive data, vulnerability scan, penetration testing, or code analysis reports of the application will be obtained and reviewed as available, prior to purchasing licenses.

Ad-hoc and emergency software releases, or releases containing immediate feature requests or bug fixes, will be scanned for vulnerabilities, and analyzed in a test environment before being released to production.

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. 54 and SP 800-30 Rev. 1
- 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, 08/01/2020, CJSD-ITSDOC-08140-5. 7

References:

MARS-E/ NIST 800-53	IRS Pub 1075	SSA	HIPAA	CJIS
RA-1	9.3.14.1	5.6	§164.308(a)(l)(i)	
RA-2	9.3.14.2		§164.308(a)(l)(ii)(A)	
RA-3	9.3.14.3		§164.308(a)(l)(ii)(B)	
RA-5			§164.308(a)(7)(ii)(E)	
RA-5 (1)				
RA-5 (2)				
RA-5 (3)				
RA-5 (5)				

Document Review and Revision Control

Version	Review Date	Author/Reviewer	Description
1.0	6/19/2019	Emily Wivell	Initial Policy
1.1	6/15/2020	Emily Wivell	Annual Renewal
1.2	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes
1.3	9/8/2022	Emily Wivell	Annual Renewal

Appendix:

None.