VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: **5.16 Information Security System and Information Integrity Policy**	**Revision Date:** **Revised Version - 6/1/20** **Current Version - 10/1/22**
Attachments/Related Documents:	Revision Number: 1.2
Name/Title of Authorizing Signature: **Jenney Samuelson, AHS Secretary**	Effective Date: 6/1/20

☒ **Trauma Informed Review**

☒ **Racial Equity Review**

Authorizing Signature: 

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security System and Information Integrity 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:

The HIPAA technical safeguards (45 C.F.R. §164.312(c}(l) and §164.312(e}(1)(2)) require AHS to implement reasonable and appropriate technical safeguards to protect and secure the electronic transmission of any health information in connection with a HIPAA-related transaction. These safeguards must protect the integrity and transmission security of electronic protected health information.

This policy assures compliance with HIPAA, as well as other 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 System and Information Integrity protocols.

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

Information Integrity Policy.

Scope:

This policy governs AHS Information Security System and Information Integrity 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 information security of AHS information systems and information integrity through the technical safeguards 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.

Flaw Remediation

AHS information systems will follow a flaw remediation framework that will integrate with

the development lifecycle and overall configuration management processes. AHS information systems will be able to identify, report on, and correct information system flaws regularly. The flaw remediation process will be centrally managed and controlled to ensure proper remediation and prevent system disruption. Flaws will be remediated in a timely fashion per the severity ranking of the identified flaw. Automated mechanisms will be used to check the status of remediations.

Malicious Code Protection and Monitoring

AHS information systems will employ malicious code protective mechanisms to prevent harmful code from entering systems. The protective mechanisms will be employed at important information system entry/exit points, workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code transported by electronic means. The protective mechanisms will be updated automatically with the latest software and signatures to ensure proper protection.

Information System Monitoring

AHS information systems will monitor system events to prevent and detect information system attacks. AHS information systems will employ the use of automated tools to support near real-time analysis and alerting of data in collected events. Both inbound and outbound communications will be monitored for unusual or unauthorized activities or conditions to prevent non-privileged users from circumventing intrusion detection and prevention capabilities.

The detection of unauthorized security changes will be integrated with AHS incident response capabilities.

Security functions will be periodically verified to ensure they are working as intended. AHS information systems will automatically notify the AHS Information Security Director of any failed security verification tests.

Security Alerts, Advisories, and Directives

Appropriate staff will promptly receive applicable security alerts, advisories, and directives form various outside organizations pursuant to protocols for:

- disseminating such information and directives internally in a timely manner, and
- implementing any necessary actions.

Security Function Verification

AHS information systems will perform verification of security functions upon system startup and restart and upon command by the administrator. The system will have the ability to notify administrators of failed security verification tests.

Intrusion Detection and Prevention

AHS information systems will utilize a wireless intrusion detection system to identify rogue wireless devices and attack attempts and potential compromises/breaches.

AHS information systems using individual intrusion detection tools will be configured to connect into a system wide intrusion detection system.

AHS information systems will employ security safeguards to protect its memory from unauthorized code execution.

Software and Information Integrity

AHS information systems will assess the integrity of software and information daily throughout the platform. This integrity verification process will detect unauthorized changes to software and information and alert the AHS Information Security Director to potential security incidents.

Spam Protection

AHS information systems will employ proper spam protection mechanisms at key system points throughout the system. Spam protection software will be centrally managed, and definitions will be updated automatically as releases are available to ensure protection against newly identified threats.

Information Input

AHS information systems will limit the ability for a user to input information into the system commensurate to their level of responsibilities and based on the principle of least privilege and separation of duties. Information will be inspected upon input for accuracy, validity, and authenticity, to prevent misuse of input fields and systems abuse.

Error Handling

AHS information systems will utilize proper structure and content of system error messages to provide information necessary for corrective actions without revealing exploited information by adversaries in error logs and administrative messages.

Information Output Handling

AHS information systems will handle and retain information within and output from the information system in accordance with applicable federal laws, Executive orders, directives, policies, regulations, standards, and operational requirements.

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, 06/01/2020, CJSD-ITS-DOC-08140-5. 7

References:

MARS-E	IRS Pub	1075	SSA	HIPAA	CJIS
SI-1	9.3.17.2		5.4	164.312(c)	5.10.4
SI-2				164.312(e)	
SI-2 (1)					
SI-2 (2)					
SI-3					
SI-3 (1)					
SI-3 (2)					
SI-4					
SI-4 (1)					
SI-4 (2)					
SI-4 (4)					
SI-4 (5)					
SI-4 (14)					
SI-5					
SI-6					
SI-7					
SI-7 (1)					
SI-8					
SI-8 (1)					
SI-8 (2)					
SI-10					
SI-11					
SI-12					
SI-16					

Document Revision Control

Version	Date	Author	Description
1.0	4/13/2020	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

Appendix:

None.