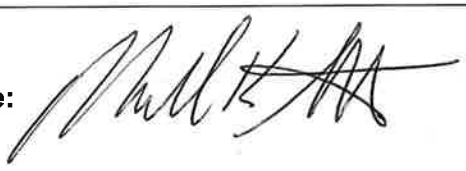
VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Planning Policy	**Policy No.** 5.19 **Revision History Date:** Replaces: **VHC-POL-PL** Current version: 3/01/20 Replaces: **DCF-POL-PL** Current version: 11/01/17
Attachments/Related Documents:	**Version Number:** 1.0
Name/Title of Authorizing Signature:	**Origination Date:**
☐**Trauma Informed Review**	

Authorizing Signature:  **Effective Date:** 10-21-20

POLICY STATEMENT:

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

Security plans relate security requirements to a set of security controls and control enhancements. Security plans describe, at a high level, how the security controls and control enhancements meet those security requirements. Security plans also contain determinations of risk to organizational operations and assets, individuals, other organizations, and if the plan is implemented as intended.

HIPAA Physical Safeguards require AHS to implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information (45 CFR § 164.310(b)).

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

SCOPE:

This policy governs Information Security protocols related to security planning 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 and updated (if necessary) at least annually.

PROTOCOLS:

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

System Security Plan (SSP)

A holistic System Security Plan (SSP) will be developed and utilized for both moderate and high-risk systems that outlines how each required security control is implemented throughout the system. Templates provided by regulatory entities such as Mars-E and the IRS will be used when applicable. The SSP will include an information security architecture which includes an architectural description, the placement/allocation of security functionality (including security controls), security-related information for external interfaces, information being exchanged across the interfaces, and the protection mechanisms associated with each interface. In addition to the information security architecture, a detailed implementation description will be provided for each control and control enhancement and may include attached documents as references if needed.

Rules of Behavior (RoB)

A Rules of Behavior (RoB) document that outlines the rules that describe the responsibilities and expected behavior of system users with regard to AHS systems and workstations will be developed, disseminated, and require all system users to read and acknowledge. The RoB will include required and prohibited behaviors for system and workstation users and potential disciplinary actions for non-compliance. The document will be reviewed and acknowledged annually by system users and signed copies will be stored.

The RoB will include explicit restrictions on the use of social media/networking sites and posting organizational information on public websites.

Privacy Impact Assessment (PIA)

Privacy Impact Assessments (PIA) will be performed on AHS information systems to determine if confidential information collected within the information systems are adequately protected. The PIA will be actively maintained and submitted as needed. At a high level, the PIA requirements include the following:

- The specific purpose of the AHS's use of a third-party website or application
- Any confidential information that is likely to become available to AHS through public use of a third-party website or application
- AHS's intended or expected use of confidential information
- With whom AHS will share confidential information
- Whether and how AHS will maintain confidential information, and for how long
- How AHS will secure confidential information that it uses or maintains
- What other privacy risks exist and how AHS will mitigate those risks
- Whether AHS's activities will create or modify a "system of records" under the Privacy Act of 1974.

Security Activities Planning

The AHS Information Security Director will ensure that security activities are planned to minimize impact on system users.

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
PL-1 PL-2 PL-2 (3) PL-4 PL-4 (1) PL-8	9.3.12.2		§164.310(b)	

(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.