VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Personnel Policy	**Policy No.** 5.25 **Revision History Date:** Replaces: DCF-POL-PS Current version: 10/16/2017
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 Personnel 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:

The HIPAA Security Rule administrative safeguards for workforce clearance procedures requires AHS to implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate (45 CFR §164.308(a)(3)(ii)(B)).

This policy follows the National Institute of Standards and Technology (NIST) SP 800-53 Rev.4 framework. The purpose of this policy is to help alleviate security risks brought on by AHS personnel. It

ensures AHS personnel fulfill the screening criteria set up by AHS and also ensures third-party personnel follow the same security criteria.

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

SCOPE:

This policy governs Information Security protocols related to personnel 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 personnel requirements.

Position Risk Designation

- A criticality/sensitivity risk designation will be assigned to all organizational positions.
- Appropriate candidate screening criteria for filling those positions will be established.
- Risk designations for all organizational positions will be reviewed and updated, as necessary.

Personnel Screening

- Individuals will be screened prior to authorizing access to AHS information systems.
- Individuals will be re-screened as necessary for the position risk rating.
- When an employee moves from one position to another, the higher level of clearance will be adjudicated.

Personnel Termination

Upon termination of employment:

- Information system access will be disabled.
- Any authenticators/credentials associated with the individual will be terminated.
- Exit interviews that include a discussion of non-disclosure of information security and privacy information will be conducted.
- All security-related AHS information system related property will be retrieved.
- Access to AHS information and information systems formerly controlled by the terminated individual will be retained.
- Defined personnel or roles will be notified within one business day.
- Employees terminated for cause will be immediately escorted out of the organization.

Personnel Transfer

- Ongoing operational needs for current logical and physical access authorizations to information systems/facilities when individuals are re-assigned or transferred to other positions within AHS will be reviewed and confirmed.
- Access authorizations will be modified as needed to correspond with any changes in operational need due to personnel re-assignment and/or transfer.

Access Agreements

- Access agreements for AHS information systems will be in place and documented.
- Individuals who require access to AHS information systems will acknowledge (paper or electronic) appropriate access agreements prior to being granted access.
- Access agreements will be reviewed and updated at least annually.

Third-Party Personnel Security

- Personnel security requirements, including security roles and responsibilities for third-party providers will be established.
- Third-party personnel will comply with AHS personnel security policies and procedures.
- Personnel security requirements will be documented.
- Third-party providers will notify the Contracting Officer or Contracting Officer's Representatives (via the roster of contractor personnel) of any personnel transfers or terminations of third-party personnel who possess AHS credentials and/or badges, or who have information system privileges within fifteen (15) calendar days.
- Third-party personnel will be monitored for compliance with this policy.

Personnel Sanctions

- All employees share responsibility for ensuring confidentiality of information systems and information contained therein. Employees caught violating this AHS policy may be subject to sanctions determined by State and Agency employment policies.

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
PS-1 PS-2 PS-3 PS-6 PS-7 PS-8	9.3.13.1 9.3.13.2 9.3.13.3 9.3.13.6		§164.308(a)(3)(ii)(B)	5.12.1

(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.