VERMONT
AGENCY OF HUMAN SERVICES

# State of Vermont
# Agency of Human Services (AHS)

| | |
|---|---|
| **Policy Title: 5.18 Information Security Awareness and Training Policy** | **Revision Date:**<br>Revision: 10/21/20<br>Current Version: |
| **Attachments/Related Documents:** | **Revision Number:** 1.1 |
| **Name/Title of Authorizing Signature: Jenney Samuelson, Interim AHS secretary** | **Effective Date:** 1/1/22 |
| ☒ **Trauma Informed Review**<br>☒ **Equity Review** | |

**Authorizing Signature:** 

## POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Awareness and Training Program 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 for Administrative Safeguards (45 C.F.R. §164.308(a)(5) requires AHS to implement a security awareness and training program for all members of its workforce (including management).

This policy details how AHS complies with HIPAA and Federal information security standards for implementing and maintaining a Security Awareness and Training Program.

This policy follows the National Institute of Standard and Technology (NIST) SP 800-53 Rev.4 framework. The purpose of this policy is to establish Information security awareness and training protocols.

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

## DEFINITIONS:

*AHS Workforce* – includes employees, volunteers, trainees, and other persons whose conduct, in the performance of work for AHS, is under the direct control of AHS, whether or not they are paid by AHS.

*User* – includes the AHS Workforce and other individuals granted access to confidential data in AHS information systems.

## SCOPE:

This policy governs Information Security protocols related to establishing a Security Awareness and Training Program and implementation of associated standards and procedures.

## ROLES AND RESPONSIBILITIES:

**AHS Secretary** – Responsible for performing 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 a Security Awareness and Training Program and associated security standards and procedures to meet the following Awareness and Training requirements to ensure that all Users are made aware of their responsibility to protect confidential data and AHS information systems.

If a minimum requirement in the information security awareness and training standards and procedures cannot be met, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

### General User Training

The Security Awareness and Training Program will serve as the fundamental security training for all Users. The training will include the following topics: general information security, general awareness, fraud, role-based training, security incident reporting, and identifying insider threats. Additional role-based trainings will be developed and added as needed to meet additional regulatory compliance or business needs. The primary training delivery system will be an online web-based platform; however, a variety of methods will be used to deliver Security Awareness Training to Users regularly throughout the year. Methods of delivery may include posters, newsletters, and emails.

The Security Awareness and Training Program will include requirements for developing and administering User training, including tracking compliance, notifying Users when training is due, and ensuring that all Users will sign an acknowledgement form upon completion of their initial information security training and annually thereafter.

### Training System Requirements

The Security Awareness and Training Program will utilize a web-based training system that provides the following functionality:

- Video and text-based training materials
- Training comprehension tests
- Tracking of training activities
- Auditing of training completion for users
- Ability to upload and store signed training documents
- Retention of training activities and records

### Training Frequency and Completion Requirements

The Security Awareness and Training Program will ensure:

- All Users will receive necessary training timely and before system IDs are issued when required.
- All Users will receive annual Security Awareness and Training refresher courses.
- The accounts of Users not in compliance with Security Awareness and Training requirements will be disabled until requirements have been completed.

### Training Review

In addition to initial User training, User trainings will be audited annually to ensure completion and adherence to requirements set forth by the State of Vermont.

### Retention of Training Records

The training system will store User Security Awareness and Training records for a minimum of five years or as otherwise required by law.

### Role-Based Training

The Security Awareness and Training Program will include opportunities to create role-based customized training courses for specific individuals or groups of Users. Customized role-based trainings will be developed with managers and subject matter experts and will be made available to designated Users. Customized role-based trainings will be required for Users who manage, administer, operate, or design IT systems, that is commensurate with their level of expertise. Role-based training will occur at the same frequencies described above.

### Curriculum Updates

The Security Awareness and Training Program will be maintained to ensure the training curriculum is up-to-date and includes topics that affect AHS's industry, operating environment, and successful or unsuccessful attempts by adversaries to obtain information from employees.

A full curriculum review of all training materials will be performed annually.

## 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 |
|---|---|---|---|---|
| AT-1<br>AT-2<br>AT-2 (2)<br>AT-3<br>AT-4 | 9.3.2.1<br>9.3.2.2<br>9.3.2.3<br>9.3.2.4 | 5.10 | §164.308(a)(1)(ii)(C)<br>§164.308(a)(2)<br>§164.308(a)(5)(i)<br>§164.308(a)(5)(ii) | 5.2.1<br>5.2.1.1<br>5.2.1.2<br>5.2.1.3<br>5.2.1.4<br>5.2.2 |

| Document Version Control | | | |
|---|---|---|---|
| **Version Number** | **Version Effective Date** | **Author** | **Description** |
| 1.0 | 10/21/2020 | Emily Wivell | Initial Version |
| 1.1 | 10/21/2021 | Emily Wivell | Annual renewal and conforming changes |

## APPENDIX:

None.