VERMONT
AGENCY OF HUMAN SERVICES

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

| | |
|---|---|
| **Policy Title: Information Security System and Services Acquisition Policy** | **Policy No.** 5.22<br>**Revision History Date:**<br>Replaces: VHC-POL-SA<br>Current version: 03/01/2020<br>Replaces: DCF-POL-SA<br>Current version: 11/01/2017 |
| **Attachments/Related Documents:** | **Version Number:**<br>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 System and Services Acquisition 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:

This policy follows the National Institute of Standards and Technology (NIST) SP 800-53 Rev.4 framework. The purpose of this policy is to ensure vendors follow the same security requirements to which the state is subject and security documentation for Information Systems is completed and periodically reviewed and updated. It also ensures software is developed with security requirements embedded. These requirements are applicable to both state and vendor software developers.

This policy details how AHS complies with Federal information security standards for implementing and maintaining an information security system and services acquisition policy.

## SCOPE:

This policy governs Information Security protocols related to system and services acquisition 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 system and service acquisition requirements.

### Allocation of Resources

Information security will be included in the information system and project management processes and ensure proper resources are available to protect systems and processes. Information security will be included in capital planning and investment control processes.

### System Development Lifecycle

A defined system development life cycle (SDLC) will be used to manage the information system that incorporates information security considerations, defines roles and responsibilities, identifies individuals having information system security roles and responsibilities and integrates the security risk management process throughout the development process.

### Development and Security

Information system development will include configuration management as a core component of system development. Additionally, Information Security engineering principles will be included in all phases of the SDLC Information Security personnel will be required to work with developers to ensure that security testing and risk mitigation is included in the SDLC

Developers of the information system, system component, or information system service will provide functional property, design, and implementation information of security controls to be employed. The developer of the information system, system component, or information system service will identify early in the SDLC, the functions, ports, protocols, and services intended for organizational use. Static code analysis will be conducted prior to promotion to the production environment, and results documented, to identify common flaws.

## Acquisition Process

Information system acquisition contracts will include requirements and/or specifications, explicitly or by reference, based on an assessment of risk and in accordance with applicable laws and regulations.

## Information System Documentation

System documentation will be developed, maintained, and protected regarding system security configuration, maintenance, installation, known vulnerabilities, and provide this documentation for administrators. User documentation will be provided that includes user-accessible security relevant features, acceptable methods of user interaction, and user responsibilities. All documentation will be updated annually and made available as needed.

## Software Controls

Software usage will be monitored to ensure approved software is used and tracked to ensure compliance with contract agreements and copyright laws. The sharing, distribution, display, performance, or reproduction of any copyrighted work or software will be prohibited. Users will be prohibited from downloading or installing unauthorized software.

## External Information Services

**External Information Services will comply with all applicable state and federal security requirements related to confidential information.**

Prior to the acquisition or outsourcing of information security services:

- External information system service providers will identify the functions, ports, protocols, and other services required for the use of such services.
- External information system service providers will not be able to access, receive, process, store, transmit, or dispose of confidential information by or through information technology systems located offshore—outside of the United States territories, embassies, or military installations.
- A risk assessment will be conducted.
- The AHS Information Security Director will notify and when applicable seek approval from federal agencies of plans to outsource before the contract is executed.
- Agreements such as business association agreements and IRS 1075 language must be included in any contractual mechanisms.

After the acquisition or outsourcing of information security services:

- External information system service providers will identify the functions, ports, protocols, and other services required for the use of such services.
- External information system service providers will comply with AHS information system security requirements and associated requirements, such as NIST, MARS-E, HIPAA, SSA, CJIS, IRS Pub 1075, and CMS.

- Security and privacy control compliance by external information system service providers will be monitored on an ongoing basis.

### Unsupported System Components

System components will be replaced when support for the component is no longer available. Approval and documentation will be needed for the continued use of unsupported system components.

### FTI Data

The use of non-agency-owned information systems, system components, or devices that receive, process, store, or transmit FTI is prohibited unless explicitly approved by the IRS Office of Safeguards.

## 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 |
|---|---|---|---|---|
| SA-1<br>SA-2<br>SA-3<br>SA-4<br>SA-4 (1)<br>SA-4 (2)<br>SA-4 (9)<br>SA-5<br>SA-8<br>SA-9<br>SA-9 (1)<br>SA-9 (2)<br>SA-9 (5)<br>SA-10 | 9.3.5.10<br>9.3.15.5<br>9.3.15.7 | | | |

| | | | | |
|---|---|---|---|---|
| SA-11<br>SA-11 (1)<br>SA-22 | | | | |

(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.