VERMONT
AGENCY OF HUMAN SERVICES

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

| | |
|---|---|
| **Policy Title: Information Security Identification and Authentication Policy** | **Policy No.** 5.21<br>**Revision History Date:**<br>Replaces:<br>VHC-POL-IA<br>Current Version: 03/01/20<br>Replaces:<br>DCF-POL-IA<br>Current Version: 10/16/17 |
| **Attachments/Related Documents:** | **Version Number:**<br>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 Identification and Authentication 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:

HIPAA Technical Safeguards require AHS to: 1) implement unique user identification specifications that assign a unique name and/or number for identifying and tracking user identity (45 CFR § 164.312(a)(1));

and 2) implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed (45 CFR § 164.312(d)).

This policy details how AHS complies with Federal information security standards for implementing and maintaining an information security Identification and authentication policy.

## SCOPE:

This policy governs Information Security protocols related to information security identification and authentication 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:

User identification is a way to identify a specific user of an information system, typically by name and/or number. A unique user identifier allows AHS to track specific user activity when that user is logged into an information system. User Identification enables AHS to hold users accountable for functions performed on information systems with Electronic Protected Health Information (EPHI) when logged into those systems. User Authentication ensures that a person is in fact who he or she claims to be before being allowed access to EPHI. This is accomplished by providing proof of identity.

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

## Identification and Authentication

### Identification and Authentication (Organizational Users)

- AHS information systems will uniquely identify and authenticate agency users and devices (or processes acting on behalf of users).
- Multifactor authentication for remote access to AHS Information Systems will be implemented
- Multifactor authentication for local access to system administrator accounts will be implemented

## Device Identification and Authentication

- The identity of AHS information system devices will be uniquely identified and authenticated before establishing a remote network connection

## Identifier Management

- Authorization will be obtained prior to assigning or creating an individual, group, role, or device identifier or account.
- A unique identifier will be used
- The unique identifier will be assigned to the intended individual, group, role, or device
- Inactive or terminated user credentials will be archived
- A process will be developed for validating system users who request reinstatement of user credentials for those suspended or revoked by AHS information systems
- Identifiers will not be reused for a minimum of 2 years
- Identifiers will be disabled after sixty (60) days or less of inactivity
- Identifiers and accounts will be disabled after employee transfer or termination

### Authenticator Management

- As part of the initial authenticator distribution the identity of the individual, group, role, or device receiving the authenticator will be verified
- Initial authenticator content will be defined and established
- Authenticators will ensure sufficient password strength for their intended use
- Administrative procedures will be established for initial authenticator distribution, lost/compromised or damaged authenticators, and for revoking authentication
- Default authenticators will be changed prior to AHS information system installation into production state
- Minimum and maximum lifetime restrictions and reuse conditions for authenticators will be established
- Authenticators will be changed per a predetermined time period, based on type of authenticator
- Authenticator content will be protected from unauthorized disclosure and modification
- Authenticators for group/role accounts will be changed when membership to those accounts change
- AHS information systems will store and transmit only encrypted passwords
- Unencrypted static authenticators will not be embedded in applications, scripts, or stored on function keys

### Authenticator Feedback

- AHS information systems will obscure feedback of authentication information during the authentication (logon) process to protect the information from possible exploitation/use by unauthorized individuals

### Cryptographic Module Authentication

- AHS Information systems will ensure that authentication to a cryptographic module meets the requirements of applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance for such authentication.

Identification and Authentication (Non-Organizational Users)

- AHS information systems will uniquely identify and authenticate non-organizational users (or processes acting on behalf of non-organizational 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 |
|---|---|---|---|---|
| IA-1<br>IA-2<br>IA-2 (1)<br>IA-2 (2)<br>IA-2 (3)<br>IA-2 (8)<br>IA-2 (11)<br>IA-3<br>IA-4<br>IA-5<br>IA-5 (1)<br>IA-5 (2)<br>IA-5 (3)<br>IA-5 (7)<br>IA-5 (11)<br>IA-6<br>IA-7<br>IA-8 | 9.3.7.1<br>9.3.7.2<br>9.3.7.3<br>9.3.7.4<br>9.3.7.5<br>9.3.7.6<br>9.3.7.7<br>9.3.7.8 | 5.3 | 164.312(a)(1)<br>164.312(a)(2)(i)<br>164.312(d) | 5.6.3.1<br>5.10.1<br>5.12.2<br>5.12.3<br>5.13.6 |

(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.