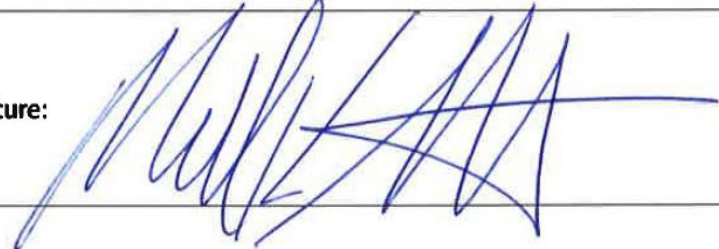# State of Vermont
Agency of Human Services (AHS)

Policy Title: 5.03 Information Security Access Control Policy	Revision Date: Revised Version – 5/1/20 Current Version – 9/1/21
Attachments/Related Documents:	Revision Number: 1.1
Name/Title of Authorizing Signature: Michael K. Smith, AHS Secretary	Effective Date: 10/23/18
☒ Trauma Informed Review ☒ Equity Review	

Authorizing Signature:

POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Access Control Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS) with all applicable State and Federal Laws, regulations, or policies.

BACKGROUND:

The HIPAA Information Access Management standard (45 CFR § 164.308(a)(4)) requires AHS to implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights. This policy assures compliance with HIPAA, as well as other state and federal laws and regulations relating to Information Security Access Controls, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

Access controls provide users with rights and/or privileges to access and perform functions using information systems, applications, programs, or files. Access controls should enable authorized users to access the minimum necessary information needed to perform their job functions. Rights and/or privileges should be granted to authorized users based on HIPAA standards.

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 Access Control protocols for AHS information systems.

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

DEFINITIONS:

Access Control —The process of granting access to information technology (IT) system resources only to authorized users, programs, processes, or other systems.

Unauthorized Access[1]— A person gains logical access without permission to a network, system, application, data, or other resource.

SCOPE:

This policy governs AHS Information Security Access Control and applies to the development and implementation of associated standards and procedures.

ROLES AND RESPONSIBILITIES:

AHS Secretary – Responsible for making a final review and approval of this policy.
AHS Policy Committee – Responsible for making final review of this policy.
Chief Information Security Officer – Responsible for:
- reviewing and approving this policy prior to AHS Policy Committee.
- reporting all compliance-related activities pertaining to this policy to the AHS Secretary.

AHS Information Security Director – responsible for:
- creating procedures and standards to meet the requirements established in this policy and incorporating state-wide procedures and standards as applicable;
- reporting all matters pertaining to AHS's compliance with this policy to the CISO; and ensuring that this policy is reviewed, and updated (if necessary), at least annually.

PROTOCOLS:

---

[1] NIST SP 800-82 Rev.2 (NIST SP 800-61) Defines Unauthorized Access as: "A person gains logical or physical access without permission to a network, system, application, data, or other resource." Since this policy only addresses access to a network, system, application, data, or other electronic resources, 'physical access' is omitted from the definition.

General

The AHS Information Security Director will establish standards and procedures to ensure access control through Account Management, Access Enforcement, System Access, and Session Control.

If an AHS information system cannot be configured to meet the minimum access control standards and procedures, the AHS Information Security Director will document an exception, receive approval from the Authorizing Official, and add the exception to the AHS risk register.

Account Management

Account Management standards and procedures will:

1) Include a system and user role matrix that documents the capabilities and permissions of each user and administrative account type in each system;

2) Require all accounts to follow the principle of least privilege and at a minimum;

- o Permit accounts to be provisioned with only the necessary privileges for the associated user, group, or service to perform their assigned role or function, and nothing more;
- o Provide that any changes of privileges to any type of user account must be reviewed and approved in advance by a designated official;
- o Prohibit actions without identification or authentication;
- o Ensure that any actions permitted without identification or authentication have documented approval and rationale behind the decision; and
- o Ensure that information sharing follows least privilege and that information is shared only with another person or system that they/it are authorized to view, process, or handle.

3) Require all accounts to adhere to proper separation of duties and at a minimum:

- o Ensure that roles and responsibilities are clearly be defined so that no one person has too much authority over access, modification, or destruction of sensitive information; and
- o Ensure that other privileged account roles are separated to prevent collusion and privilege abuse, such as having privileges to manage access control be separate from administering audit functions, or the ability to process and approve critical business functions (e.g. payroll).

4) Require that appropriate processes are used to support the management of accounts and that organizational standards are established for creating, enabling, modifying, disabling, and removing information system accounts;

5) Ensure that user, service, and system accounts undergo a periodic privilege review to ensure that accounts have been provisioned according to established requirements, and do not violate least privilege or separation of duties and that accounts that are no longer in use are disabled or removed, as appropriate; and

6) Require that accounts are configured to include access limitations for lockouts, invalid login attempts, and minimum time periods for locked accounts.

Access Enforcement

Access Enforcement standards and procedures will prohibit unauthorized access and will include at a minimum:

- Appropriate access enforcement mechanisms such as access control lists, access control matrices, encryption; and
- Specifications for deploying those mechanisms at the information system level or the application level.

System Access

System Access standards and procedures will:
- Establish acceptable methods of system access, including remote, wireless, and mobile device access;
- Prohibit the use of external information systems to access AHS information systems or data, unless an exception is specifically documented and approved by a designated official;
- Require that, as part of the logon process, the system displays an approved system use notification message or banner, before granting access to the system, that provides privacy and security notices consistent with applicable federal and state requirements;
- Establish and document approved system uses that can be performed without authentication or authorization and require that such uses are explicitly controlled by named individuals who are responsible for defining what anonymous users can do on the system and ensure that publicly displayed data is screened for sensitive information; and
- Ensure that only authorized staff are allowed to post information on publicly accessible information systems and that all content to be posted publicly is reviewed and approved in advance by a designated official.

Session Control

Session Control standards and procedures will include specifications and mechanisms for concurrent session control and session locking.

ENFORCEMENT:

The AHS Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines, protocols or procedures 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
AC-1	9.3.1.1	5.3	§164.308(a)(3)(i)	5.5.1
AC-2 (1)	9.3.1.2		§164.308(a)(3)(ii)(A)	5.5.2
AC-2(2)	9.3.1.4		§164.308(a)(3)(ii)(B)	5.5.2.1
AC-2(3)	9.3.1.5		§164.308(a)(3)(ii)(C)	5.5.3
AC-3	9.3.1.6		§164.308(a)(4)(i)	5.5.5
AC-4	9.3.1.7		§164.308(a)(4)(ii)(B)	5.5.6
AC-5	9.3.1.9		§164.308(a)(4)(ii)(C)	
AC-6	9.3.1.10		§164.310(b)	
AC-6 (1)	9.3.1.12		§164.310(c)	
AC-6 (2)			§164.312(a)(1)	
AC-6 (5)			§164.312(a)(2)(i)	
AC-6 (9)			§164.312(a)(2)(ii)	
AC-7			§164.312(d)	
AC-8				
AC-10				
AC-11				
AC-12				
AC-14				
AC-17				
AC-17(3)				
AC-17(4)				
AC-18				
AC-19				
AC-20				
AC-21				
AC-22				

Document Review and Revision Control			
Version	**Review Date**	**Author/Reviewer**	**Description**
1.0	11/19/2019	Emily Wivell	Revised Policy 5.03 Effective
1.1	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes

APPENDIX:

None.