VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: 5.14 Information Security System and Communications Protection Policy	Revised Version – 5/1/20 Current Version – 10/1/22
Attachments/Related Documents:	**Revision Number: 1.1**
Name/Title of Authorizing Signature: **Jenney Samuelson, AHS Secretary**	Effective Date: 5/1/20

☒ **Trauma Informed Review**
☒ **Racial Equity Review**

Authorizing Signature:

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security System and Communications Protection 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.

Background:

The HIPAA Security Rule for the Protection of Electronic Protected Health Information (ePHI) requires AHS to implement technical safeguard standards for Access Control (data at rest) and Transmission Security (data in transit). Per the HIPAA Access Control implementation specifications (45 C.F.R. §§164.312(a)(2)(iv)), AHS is required to implement a mechanism to encrypt and decrypt ePHI. Per the HIPAA Transmission Security implementation specifications (45 C.F.R. §§164.312(e)), AHS is required to implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network, ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of, and encrypt ePHI whenever deemed appropriate

This policy details how AHS complies with HIPAA and Federal information security standards for how AHS systems and network information is protected in transit or at rest. This policy assures compliance with HIPAA, as well as other state and federal laws relating to Information Security Systems and Communications Protection, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

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 System and Communication Protection protocols.

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

Definitions:

Confidential Data - includes social security numbers, personal financial information, debit/credit card numbers, personally identifiable health information, electronic protected health information, and any other data that is identified by law, regulation, policy, or practice as confidential.

Scope:

This policy governs Information Security protocols related to the protection of AHS Systems and Communications 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 a final review of this policy.

Chief Information Security Officer – Responsible for reviewing and approving this policy prior to AHS Policy Committee. The CISO must 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:

- documenting system interconnections,
- managing IT security networking encryption,

- 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 standards and procedures to meet the following specifications to ensure system and communication protection through System Connections, System Protections and Communication Restrictions, and Encryption.

If an AHS information system cannot be configured to meet the minimum information security system and communication protection 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.

System Connections

Wireless Access

All wireless access for AHS information systems must follow AHS standards and guidance, including explicit authorization prior to allowing connections.

Information Shared resources

Information systems must be configured to prevent unauthorized and/or unintended information transfer via shared system resources. AHS must ensure that system resources shared between two (2) or more users are released back to the information system and are protected from accidental or purposeful disclosure.

Restrictions on external system connections

Information systems must be configured to only accept connections from authorized information systems from outside the organization.

External Telecommunications Services

Each external telecommunication service must have its own managed interface and traffic flow policy. Any exceptions to the traffic flow policies must be approved and documented.

System Protections and Communication Restrictions

Deny by Default

Network communications traffic must be denied by default and allowed by exception.

Denial of Service Protection

AHS Information systems must be designed to be resilient to Denial of Service (DoS) attacks to ensure the availability of AHS systems and data to users.

Boundary Protection

The boundary, or the outermost network devices owned or hosted by AHS, must be configured using least functionality, meaning configured to use only essential ports and services. Boundary protection devices must be configured to fail securely in the event of an operational failure. Additional measures, outlined below, may also be employed to further ensure that only desired traffic is permitted into or outside the organization:

- Host-based boundary protections must be implemented.
- Communications across the external boundary and key internal boundaries must be monitored and controlled using the philosophy of “deny by default /allow by exception.” This philosophy requires that managed interfaces must be configured to deny network communications traffic by default and only permit network communications traffic by exception (such as whitelisting).
- Sub networks must be utilized for any publicly accessible system components that are physically or logically separated from internal networks.
- Only approved managed interfaces may be used to connect systems to external networks.

Collaborative Computing Devices

Collaborative computing devices are prohibited unless explicitly authorized in writing. If confidential information is accessible through a collaborative computing device, the following controls must be in place:

- remote activation must be prohibited
- a documented approved exception must be in place
- an explicit indication of use to users physically present at the device must be shown

Mobile Code

Acceptable and unacceptable mobile code must be defined and documented in the systems and communications protection standard. AHS Information Security Director must define usage restrictions for acceptable mobile code and monitor the use of mobile code within the information system.

VOIP

Any utilization of VOIP must follow AHS usage restrictions and implementation guidance based on the potential to cause damage to the information system if used maliciously; and
authorizes, monitors, and controls the use of VoIP within the information system.

Session Authenticity
Authenticity of communications sessions must be protected (e.g. by invalidating session identifiers upon logout or session termination).

Network Disconnect
Information systems must terminate the network connection at the end of a session.

Spam Protection
Spam protection mechanisms at information system entry and exit points must be used to detect and act to address any unsolicited messages. These protection mechanisms must be centrally managed and configured to automatically update.

Application Partitioning
Information systems must be partitioned, and access be strictly controlled. Proper application partitioning will be implemented to separate user functionality of systems from information systems management and administration (e.g. separating web services from database management systems). The method of application partitioning may vary depending on the system design and functionality.

Process Isolation
A separate execution domain must be maintained for each executing process.

Encryption

Data at Rest

Data at rest refers to information that is not being actively processed, handled, or transmitted; it is simply being stored. AHS must ensure that all information systems that are used to store confidential data are protected at rest by using encryption mechanisms. Examples where encryption should be used include:

- **Backups** – Includes backup hard drives, CD/DVD/BLU-RAY, tape backups, etc.
- **Laptops & Workstations** – Hard disc drives (HDDs) and solid-state drives (SSDs).
- **Mobile devices** – phones, tablets, etc.
- **Servers** – HDDs and SSDs
- **Storage devices** – Network attached storage (NAS), Direct attached storage (DAS), Storage Area Networks (SAN), and other similar devices and technologies should be encrypted to protect confidential data
- **Portable storage** – Flash media, pen drives, etc.
- **Databases** – Database encryption mechanisms should be leveraged to provide additional protection against access to confidential information if a system becomes compromised

- **Files/folders** – File and folder level encryption should be leveraged as necessary to protect specific files or folders that contain confidential information.

Data in Transit

Data in transit refers to information that is in motion or being sent (transmitted) from a source to a destination. When transmitting confidential information AHS must ensure that encryption mechanisms are used to encrypt either the data, or the transportation protocol. Examples where encryption must be used when transmitting confidential information include:

- **Email** – Encrypting the text and/or the attachments of an email message.
- **Internal network traffic** – Encrypted traffic between different internal networks, systems, or devices that does not leave organizational network boundaries or perimeters.
- **External network traffic** – Encrypted traffic between AHS and an external entity.
- **Virtual Private Network (VPN)** – Using encrypted network tunneling protocols to extend the enterprise network, or services hosted on the enterprise network, across a public network such as the internet.
- **Web services** – Any services hosted on a website or web-based application between the client (a user, information system or service) and the host (typically the web server/application).

Standards/levels of encryption

The strength of encryption used (encryption protocol, key length, etc.) must correspond with the sensitivity of the data transmitted Encryption levels and standards must be periodically reviewed to ensure continued compliance with applicable legal obligations associated with the data such as with existing contracts, or legal and regulatory requirements for various types of data (PCI, ePHI, PII, etc.). If public key certificates are used, they must be obtained from an approved certificate service provider. FTI and MARS-E data must be protected using FIPS 140-2 validated encryption mechanisms.

Key Management

Key management processes and procedures must be centrally managed. Centralized Key Management processes will include secure creation, storage, revocation, renewal, and disposal of encryption keys.

Public key certificates will be issued using an approved certificate policy or obtained from an approved provider.

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
SC-1	9.3.16.5	5.8	45 C.F.R. §§ 164.308(a)(1)(ii)(D), 164.312(a)(1), 164.312(a)(2)(iv) 164.312(b), 164.312(e); 45C.F.R. §164.308(a)(6)(i)	5.10
SC-2	9.3.16.6			
SC-4	9.3.16.15			
SC-5				
SC-7				
SC-7 (3)				
SC-7 (4)				
SC-7 (5)				
SC-7 (7)				
SC-7 (12)				
SC-7 (13)				
SC-7 (18)				
SC-8				
SC-8 (1)				
SC-8 (2)				
SC-10				
SC-12				
SC-12 (2)				
SC-13				
SC-15				
SC-18				
SC-19				
SC-20				

SC-21
SC-22
SC-23
SC-28
SC-32
SC-39

Document Revision Control

Version	Date	Author	Description
1.0	2/24/2020	Emily Wivell	Initial Version
1.1	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes

Appendix:

None.