

AHS Policy Title: 5.17 Information Security Physical and Environmental Protection Policy

Policy Information

Revision Date:

02/21/2023

Revision Number:

1.3

Attachments/Related Documents:

none


Effective Date:

07/01/2020

Trauma Informed Review

Racial Equity Review

Authorizing Signature:



Jenney Samuelson,
Agency of Human Services Secretary

Policy Statement:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Physical and Environmental 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, 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 Physical Safeguards requires AHS to implement policies and procedures to limit physical access to its electronic information systems and the facilities in which they are housed, while ensuring that properly authorized access is allowed (45 C.F.R. §164.310(a)). Physical Safeguards include protecting electronic information systems and related buildings and equipment from natural and environmental hazards and unauthorized intrusion (45 C.F.R. §164.302).

This policy details how AHS complies with HIPAA and Federal information security standards for physical safeguards including controlling physical access to and providing environmental protections for AHS information systems and the facilities that house them.

This policy follows the National Institute of Standard and Technology (NIST) SP 800-53 Rev.5 framework. The purpose of this policy is to establish Information Security Physical and Environmental Protection protocols.

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

Definitions:

Contractor – an individual performing work on behalf of the State of Vermont pursuant to a contract with an assigned workstation in the facility.

Restricted Areas - locations where AHS' confidential information is used, disclosed, stored, processed, or transmitted.

Data Center- a Restricted Area where AHS information systems and associated components are located, operated, or managed.

Employee – A full time, part-time, or temporary employee or authorized intern of the State of Vermont with an assigned workstation in the facility or with authorized access to the facility.

Visitor – an individual on site at a State of Vermont facility who does not have an assigned workstation in the facility and is present for a limited specific purpose, such as a meeting or other event, vendor delivery, facility maintenance, or other authorized purpose.

Public Areas – locations within AHS facilities where confidential information is not used, disclosed, stored, processed, or transmitted.

Scope:

This policy governs Information Security protocols related to Physical and Environmental Protection 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 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 security standards and procedures to meet the following physical and environmental controls to limit physical access to AHS information systems and the facilities that house them, to ensure AHS information systems are protected in their physical environment, and to ensure that properly authorized access is allowed.

If an AHS information system cannot be configured to meet the minimum information security physical and environmental 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.

Physical Security Controls

Physical Access Authorizations

Access to AHS facilities will be consistent with building management requirements established by the Department of Buildings and General Services (BGS).

A list of individuals with authorized access to the facility where AHS information systems reside will be maintained. Access credentials will be authorized based on position and role. The authorized access list must be reviewed at least once every 180 days. Access will be revoked when an individual no longer requires it. A Restricted Area must be used to control access to systems containing confidential information.

All Employees, Contractors, and other authorized individuals will be issued badges/keys by BGS to gain access to AHS facilities (both for general access from outside and any internal access to restricted Areas). Employee or Contractor ID badges will be worn within the building and clearly displayed at all times. Physical access will be controlled, and Employees may be required to use IDs or badges to access Restricted Areas.

Physical Access Control

AHS facilities will provide security safeguards to control access to Public Areas. Individual access authorizations will be verified before access to the facility is granted. All Visitors will be escorted and monitored.

Defined entry and exit points to facilities containing AHS data will have physical access authorizations such as badges, keys, combinations, or guards. All physical access devices will be secured. Access logs will be kept for the defined entry and exit points. Physical access devices will be inventoried at least annually. Keys or combinations will be changed at least every 365 days; sooner if they have been compromised, or individuals are transferred or terminated.

Physical access authorizations and physical security controls are required for any Restricted Areas. Individual access authorizations will be required for access to any areas with FTI data.

Visitors will not be left unattended in any Restricted Area within AHS facilities. Visitors will be escorted by an authorized Employee during their presence in Restricted Areas.

Physical access to AHS system distribution and transmission lines within AHS facilities will be controlled. Physical access to AHS information system output devices will be controlled.

Monitoring Physical Access

Physical access to AHS facilities where information systems reside will be monitored. Access logs will be kept and reviewed at least every two months, or weekly in the event of a physical security incident.

Visitor access records for AHS facilities, except those deemed public, will be maintained. Records will be kept for five years and must be reviewed at least monthly.

Access log reviews must also be performed periodically to search for anomalous activity. Anomalous activity may consist of Employees or Contractors accessing the facility during non-business hours, accessing, or attempting to access areas or facilities not consistent with their access privileges.

Alarm System

All AHS facilities will maintain an alarm system and surveillance equipment to detect and monitor any intrusions or attempts at intrusion.

Alternate Work Site

Alternate work sites may include government facilities or private residences of Employees. Alternate work sites will employ proper operational and technical information system security controls. A means for Employees to communicate with information security personnel will be provided in case of security incidents or problems. IRS Office of Safeguards requirements will be implemented at alternate work sites where FTI exists.

Data Center Environmental Controls

Fire protection/suppression

AHS facilities will maintain a fire detection and suppression system supported by an independent energy source. The system will activate automatically and notify the correct personnel and emergency responders in the event of a fire. If AHS facilities are not staffed continuously, automatic fire suppression capabilities will be utilized. Temperature and Humidity Controls AHS facilities where systems reside will monitor and control the humidity and temperature levels. There will be a process to alert personnel should these levels deviate from the acceptable range.

Power Equipment and Cabling

AHS facilities will protect power equipment and cabling from damage by allowing only authorized maintenance personnel access.

Emergency Power

AHS facilities will have a short term, uninterrupted back-up power source to facilitate the proper

shutdown of systems in the event of a power loss.

Emergency Shutoff

AHS facilities will ensure that power to all systems or system components can be easily shut off in emergency situations. Emergency power switches will be in a location that does not require personnel to approach any equipment. Physical controls will be taken to ensure unauthorized personnel do not have access to these switches.

Emergency Lighting

AHS facilities will maintain automatic emergency lighting that activates in the event of a power loss. Lighting will cover emergency exits and evacuation routes within the facility.

Water Damage Protection

AHS facilities will have master shutoff or isolation valves to prevent damage from leaking water. These valves will be accessible, well maintained, and known to authorized Employees and Contractors.

Delivery and Removal

Information system related components entering and exiting AHS facilities will be authorized, monitored, and controlled. A record will be kept of those items.

Location of Information System Components

AHS Information System Components will be positioned within AHS facilities in a way that minimizes potential damage from physical and environmental risks and minimizes the potential for unauthorized access.

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
- National Institute of Standards and Technology (NIST) SP 800-53 Rev. 5
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E), Version 2.2, September 16, 2021
- IRS Publication 1075 (Rev. 11-2021)
- 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 5.9.1, 10/01/2022, CJSD-ITS-DOC-08140-5.9.1

References:

MARS-E	IRS Pub 1075	SSA	HIPAA	CJIS
PE-1		5.13	§164.302	5.9
PE-2	PE-1		§164.310(a)(1)	5.9.1
PE-2 (1)	PE-2		§164.310(a)(2)(ii)	5.9.1.1
PE-3	PE-3		§164.310(a)(2)(iii)	5.9.1.2
PE-4	PE-4		§164.310(a)(2)(iv)	5.9.1.3
PE-5	PE-5		§164.310(c)	5.9.1.4
PE-6	PE-6			5.9.1.5
PE-6 (1)	PE-8			5.9.1.6
PE-8	PE-16			5.9.1.7
PE-9	PE-17			5.9.1.8
PE-10				5.9.2
PE-11				
PE-12				
PE-13				
PE-13 (3)				
PE-14				
PE-15				
PE-16				
PE-17				

Document Review and Revision Control

Version	Review Date	Author/Reviewer	Description
---------	-------------	-----------------	-------------

1.0	6/11/2020	Emily Wivell	Initial Version
1.1	7/6/2021	Emily Wivell	Annual Renewal and Conforming Changes
1.2	9/8/2022	Emily Wivell	Annual Renewal
1.3	02/21/2023	Emily Wivell	Annual Renewal

Appendix:

None.