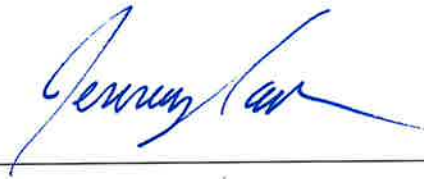


State of Vermont Agency of Human Services (AHS)

Policy Title: 5.24 Information Security Contingency Planning Policy	Revision Date: Current version: 3/1/22
Attachments/Related Documents:	Revision Number: 1.1
Name/Title of Authorizing Signature: Jenney Samuelson, Interim AHS secretary	Effective Date: 12/15/2020
<input checked="" type="checkbox"/> Trauma Informed Review <input checked="" type="checkbox"/> Equity Review	

Authorizing Signature:



POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Contingency Planning 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 administrative safeguards for contingency planning requires AHS to establish policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information (45 CFR §164.308(a)(7)(i)). As part of the federal requirements for contingency planning, AHS needs to have a data backup plan, a disaster recovery plan, and an emergency mode operations plan.

This policy also follows the National Institute of Standards and Technology (NIST) SP 800-53 Rev.4 framework. The purpose of this policy is to establish contingency planning for information systems as part of an overall organizational program for achieving continuity of operations for mission/business functions. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised.

This policy details how AHS complies with Federal information security standards for implementing and maintaining an information Security contingency Planning Policy.

SCOPE:

This policy governs Information Security protocols related to contingency planning 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 for an Information Security Contingency Policy that ensures the confidentiality, integrity, and availability of information and systems within the Agency of Human Services (AHS).

If an AHS information system cannot be configured to meet the minimum information security contingency planning 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

Contingency Plan

A contingency plan will be developed for AHS information systems to establish data backup, disaster recovery, and emergency mode operations in which:

- Business owners identify essential mission(s) and business functions and associated contingency requirements.
- Recovery objectives, restoration priorities, and metrics are identified.
- Contingency roles and responsibilities are identified, and individuals are assigned to each role with their contact information.
- The resumption of essential missions and business functions are planned for.
- Critical technical and operational assets that support essential missions and functions are identified.
- Eventual, full system restoration without deterioration of the security safeguards originally planned and implemented are addressed.

Copies of the plan will be distributed to key contingency personnel.

Contingency plan activities will be coordinated with incident handling activities and other plans such as business continuity plans, continuity of operation plans, and security incident response plans.

The contingency plan will be reviewed and updated annually or when changes are made to the information system(s).

The contingency plan will be protected from unauthorized disclosure, inspection, and modification.

Contingency Training

Contingency plan training will be provided to personnel with assigned security roles and responsibilities prior to assuming the contingency role or responsibility, and when required by information system changes, and annually thereafter.

Contingency Plan Testing

- Contingency plans for AHS information systems will be tested annually.
- Contingency plan testing activities will be coordinated with other elements responsible for related plans such as business continuity, continuity of operations, and security incident response plans.
- Contingency plan test results will be reviewed within 30 calendar days and any corrective actions will be documented and initiated.

Alternate Storage Site

- An alternate storage site will be established and will include necessary agreements to permit the storage and retrieval of AHS information system backup information.
- The alternate storage site will provide information security safeguards equivalent to that of the primary site.
- The alternate storage site will be separated from the primary storage site to reduce susceptibility to the same threats.

Alternate Processing Site

- An alternate processing site will be established and will include necessary agreements to permit the transfer and resumption of AHS information system operations.
- The alternate processing site will provide information security safeguards equivalent to that of the primary site.
- Equipment and supplies required to transfer and resume operations will be available at the alternate processing site or contracts will be in place to support delivery to the site within the recovery time objective requirements.
- The alternate processing site will be separated from the primary storage site to reduce susceptibility to the same threats.
- Alternate processing site agreements will contain priority-of-service provisions in accordance with the availability requirements (including recovery time objectives).

Telecommunications Services

- Requirements will be determined to establish alternate telecommunications services including necessary agreements to permit the resumption of the AHS Information system(s) operations necessary for essential missions and business functions and to reduce the likelihood of sharing a single point of failure with primary telecommunications services.
- Alternate telecommunications services agreement provisions will consider availability, confidentiality, integrity, quality of service, access, and priority-of-service requirements.

Information System Backup

- Backups will be conducted of user and system-level information contained in AHS Information Systems as required to support the business functions.
- Backups will be conducted of AHS information system documentation including security-related documentation as required to support the business function.
- Backups will be monitored to ensure successful completion and take corrective action if the backup did not complete successfully.
- The confidentiality, integrity, and availability of backup information at primary and alternate storage locations will be protected.

- Backup information will be tested in accordance with business requirements such as recovery time objective, and to verify media reliability and information integrity.

Information System Recovery and Reconstitution

- The recovery and reconstitution of AHS information systems will be to a known state after a disruption, compromise, or failure.
- Recovery of AHS information systems after a failure or other contingency will be done in a trusted, secure, and verifiable manner.
- AHS Information Systems will implement transaction recovery (e.g., transaction rollback and transaction journaling) for transaction-based systems (for example, database management systems and transaction processing systems).

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
CP-1	9.3.6.1		§164.308(a)(7)	
CP-2	9.3.6.2		§164.310(a)(2)(i)	
CP-2 (1)	9.3.6.3			
CP-2 (3)	9.3.6.4			
CP-2 (8)	9.3.6.5			

CP-3	9.3.6.6			
CP-4	9.3.6.7			
CP-4 (1)	9.3.6.8			
CP-6				
CP-6 (1)				
CP-6 (3)				
CP-7				
CP-7 (1)				
CP-7 (2)				
CP-7 (3)				
CP-8				
CP-8 (1)				
CP-8 (2)				
CP-9				
CP-9 (1)				
CP-10				
CP-10 (2)				

(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	12/15/2020	Emily Wivell	Initial Version
1.1	01/10/2022	Emily Wivell	Annual renewal and conforming changes

APPENDIX:

None.