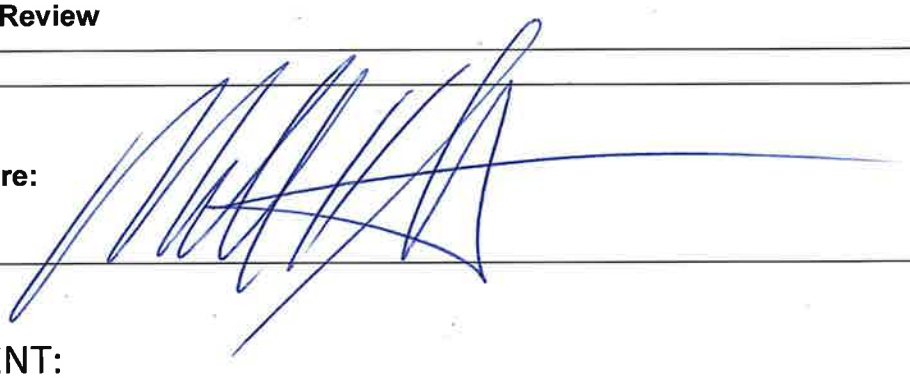
VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Information Security Incident Management Policy	**Policy No. 5.05** **Revision History Date:** Initial Version – 11/2008 Revision – 7/5/2017 Revision – 1/15/19 Current Version – 10/22/2019
Attachments/Related Documents:	**Revision Number:** 1
Name/Title of Authorizing Signature: Michael K. Smith, AHS Secretary	**Effective Date: 11/1/20**
☒Trauma Informed Review	
Authorizing Signature: 	

POLICY STATEMENT:

To establish high-level requirements, organizational responsibilities, and managerial commitment for an Information Security Incident Management 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 Laws, regulations, or policies.

BACKGROUND:

The HIPAA Security Incident Procedures standard (45 CFR § 164.308(a)(6)(i)) requires AHS to implement policies and procedures to address security incidents. The implementation specification for response and reporting (45 CFR § 164.308(a)(6)(ii)) requires AHS to identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to AHS; and document security incidents and their outcomes. This policy assures compliance with HIPAA, as well as other state and federal laws relating to information security incidents, such as those established by CMS, Internal Revenue Service, Social Security Administration, Criminal Justice Information Services, and Vermont law.

Information Security Incident Response Management includes an Incident Response Plan and related procedures and standards to assure timely detection, handling, reporting, communication, response and mitigation of information security incidents. Information Security Incident Response Management

capabilities are necessary for rapidly detecting incidents, minimizing loss and destruction, mitigating the weaknesses that were exploited, and restoring IT services.

DEFINITIONS:

Information Security Incident or Incident – means the attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system.

Information Spillage – means instances where sensitive information is inadvertently placed on information systems that are not authorized to process such information and includes accidental data transfers to lower environments.

Information system – means an interconnected set of information resources on the AHS enterprise network and includes hardware, software, information, data, applications, communications, and people.

SCOPE:

This policy governs the AHS response to an Information Security Incident and applies to the development and implementation of an Information Security Incident Response Plan ("Incident Response Plan" or "Plan") and 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 a final review of this policy.
Chief Information Security Officer (CISO) – Responsible for:

- reviewing and approving this policy prior to AHS Policy Committee;
- ensuring all Information Security Incident Response Management activities are properly integrated into the necessary information systems;
- and reporting all compliance-related activities pertaining to this policy to the AHS Secretary.

AHS Information Security Director – Responsible for:

- developing and implementing the Incident Response Plan;
- creating procedures and standards to meet the requirements established in this policy;
- convening the Incident Response Team;
- ongoing tracking and documenting of all reported security incidents;
- ensure that key personnel participate in annual incident response testing and exercises to determine the plan's effectiveness;
- document testing of incident response capabilities;
- 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.

AHS Incident Response Team – Responsible for:

- ensuring all incidents are addressed and remediated according to the Incident Response Plan and related procedures and standards.

PROTOCOLS:

Incident Response Plan

The AHS Information Security Director developed an Incident Response Plan ("Plan") to establish the procedures to identify and categorize events that occur on the AHS enterprise network and then to respond accordingly to those events. The Incident Response Plan will:

1) Identify and assign key roles and responsibilities for those responding to incidents. Key personnel will:
   a) serve on an incident response team;
   b) evaluate the severity of an event to determine whether it should be escalated to an incident (Minor and Major);
   c) enact appropriate response activities for the incident in a timely manner;
   d) participate in training activities for their assigned roles within 90 days of assuming the role, and
   e) participate in annual incident response testing and exercises.

2) Include provisions for communication and coordination of the Plan to ensure that all AHS employees are made aware of the Plan and know how to recognize and report incidents in a timely manner.

3) Include clear protocols for chain of command and internal and external communication channels to quickly and efficiently report and escalate, as appropriate. The protocols will address coordinating internal and external communications between the Incident Response Team and AHS Leadership relating to an incident.

4) Include provisions to ensure coordination across AHS departments to ensure affected departments and workforce members are aware of their associated role, if any, in implementing the Plan or responding to an incident, including initiating appropriate breach notification activities.

5) Establish the protocols for the AHS Information Security Director to convene an Incident Response Team, which will include ensuring all Incident Response Team members are aware of their roles and responsibilities for executing the plan, coordinating all technical activities associated with the incident response, and designating the incident Response Team Lead.

6) Address Information Spillage. The Plan will include each of the following steps:

   a. Identification: AHS will respond to Information Spillage by identifying the information and systems that have been affected.

   b. Notification: AHS will alert authorized Incident Response Team personnel of the Information Spillage. Any personnel that have been exposed to the spilled information will be made aware of any applicable laws, regulations or policies that govern the data.

   c. Isolation: AHS will take actions to isolate the contaminated information system or component to prevent further Information Spillage into other systems.

   d. Eradication: AHS will eradicate the Information Spillage from the contaminated information system or component. Disposition of data will be eradicated and recorded in accordance with any laws, regulations or policies.

7) Include provisions for required security breach notifications.

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; and 45 CFR 164.308(a)(6) Security Incident Procedures Standard
- Exchange Establishment Standards and Other Related Standards Under the Affordable Care Act: 45 CFR 155.260 - Privacy and security of personally identifiable information
- Centers for Medicare and Medicaid Services (CMS), Minimum Acceptable Risk Standards for Exchanges (MARS-E)
- IRS Publication 1075
- 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
- NIST Special Publication 800-61, Computer Security Incident Handling Guide
- Security Breach Notice Act, 9 V.S.A. § 2435
- Social Security Number Protection Act, 9 V.S.A. § 2440
- Document Safe Destruction Act, 9 V.S.A. § 2445
- AHS Policy 1.01 Development and Dissemination of AHS-wide Policies, Protocols, Guidelines and Procedures
- The Privacy Act of 1974, E-Government Act of 2002 (P.L. 107-347)

REFERENCES:

MARS-E/NIST 800-53	IRS Pub 1075	SSA	HIPAA	CJIS
IR-1	9.3.8.1	5.9	§164.308(a)(6)	
IR-2	9.3.8.2			
IR-3	9.3.8.3			
IR-3 (2)	9.3.8.4			
IR-4	9.3.8.5			
IR-4 (1)	9.3.8.6			
IR-5	9.3.8.7			
IR-6	9.3.8.8			
IR-6 (1)				
IR-7				
IR-7 (1)				
IR-8				
IR-9				

Document Review and Revision Control			
Version	**Review Date**	**Author/Reviewer**	**Description**
1.0	9/18/2019	Emily Wivell	Revised Policy 5.05 Effective 01/15/2019
1.1	10/01/2020	Emily Wivell	Annual Renewal and Conforming Changes