VERMONT
AGENCY OF HUMAN SERVICES

State of Vermont
Agency of Human Services (AHS)

Policy Title: Incident Response	**Revision Date:** Initial Version – 11/2008 Current Version – 7/5/2017
Attachments/Related Documents:	**Revision Number:** 5.05
Name/Title of Authorizing Signature: Al Gobeille, Secretary, AHS	**Effective Date:** 1/15/2019

Authorizing Signature:	Al J Gobeille

POLICY STATEMENT:

To ensure effective monitoring and response to all Information Technology (IT) incidents or suspected incidents by addressing all critical aspects of Incident Response (IR) and containment.

BACKGROUND:

NIST Special Publication 800-61, Computer Security Incident Handling Guide
https://csrc.nist.gov/publications/detail/sp/800-61/rev-2/final

Minimum Acceptable Risk Standards for Exchange (MARS-E), CMS, Incident Response

45 CFR 164.308(a)(6) Health Insurance Portability and Accountability Act (1996), Security Incident Procedures Standard

Security Breach Notice Act, 9 V.S.A. § 2435, the Social Security Number Protection Act, 9 V.S.A. § 2440; and the Document Safe Destruction Act, 9 V.S.A. § 2445 45 CFR 155.260 - Privacy and security of personally identifiable information.

DEFINITIONS:

CSIRT- Computer Security Incident Response Team

Event- an observable occurrence within a system or network

Security Incident- a violation or imminent threat of violation of computer security policies, acceptable use policies, or standard security practices

Reportable Security Incident- attempted or successful unauthorized access, use, disclosure, modification, or destruction of information; or interference with system operations in an information system

VERMONT
AGENCY OF HUMAN SERVICES

SCOPE:

This document applies to all Agency Departments, Divisions and Offices hereafter referred to jointly as "department". This document also applies to contractors, business associates, and other users of departmental information systems.

STANDARDS:

AHS employees and contractors accessing social security data shall be responsible for communicating reportable security incidents to the AHS Incident Response team.

The AHS Security Director shall establish an Agency IR team. The team, working with departmental IT Managers, shall develop, disseminate, review, and update AHS IR controls. The team will also develop, document, and implement procedures to effectively monitor and respond to all IT security incidents or suspected incidents by addressing all critical aspects of incident handling and response containment. The IR procedures shall be consistent with applicable laws, directives, policies, regulations, standards, and guidance.

As a result of this policy, plans and procedures shall ensure the following:

Annual training of employees and IT personnel at a level commensurate to their IR roles and responsibilities with respect to AHS information systems.

- At minimum, annual documented testing of IR capability for AHS information systems to determine the plan's effectiveness.
- Incident handling capability including preparation, identification, containment, eradication, recovery, and follow-up capabilities in response to security incidents.
- Preservation of evidence of computer crimes, computer misuse, and all other unlawful computer activities.
- Ongoing monitoring of AHS information systems.
- Ongoing tracking and documentation of all reported security incidents.
- Reporting of all IT systems incidents, or suspected incidents to the designated AHS IT Incident Response Team and state CSIRT.

COMPLIANCE:

It is the responsibility of the individual departments to ensure dissemination and review of this policy to all employees within their organizations and other associates as appropriate. Per Federal requirements, if AHS experiences or suspects a breach or loss of sensitive data or a security incident, which includes SSA provided information, they must notify the State official or delegate as designated in the agreement with the federal partner.

Social Security Administration - Social Security Data

AHS employees and contractors must notify the designated State official or delegate at AHS.PrivacyAndSecurity@vermont.gov who must then notify the SSA Regional Office Contact or the SSA Systems Security Contact identified in the agreement. If, for any reason, the responsible State official or delegate is unable to notify the SSA Regional Office or the SSA Systems Security Contact within one hour, the responsible State Agency official or delegate must report the incident by contacting SSA's National Network Service Center (NNSC) toll free at 877-697- 4889 (select "Security and PII Reporting" from the options list). The Electronic Information Exchange Partner (EIEP) will provide updates as they become available to the SSA contact, as appropriate.

State officials may be further required to report a suspected breach of loss of sensitive data or a security incident which includes SSA provided information to the Vermont Attorney General (VT AGO) (per 9 V.S.A. § 2435), to CMS (45 C.F.R. §155.260(a)(3)(viii)), and provide security breach notification(s) to impacted consumers (per 9 V.S.A. § 2435).

Providing Security Breach Notice:

State may also be required to notify a consumer that there has been a security breach following discovery or notification to the data collector of the breach.

ENFORCEMENT:

The Office of the Secretary may initiate reviews, assessments or other means to ensure that policies, guidelines or standards are being followed.