State of Vermont

Incident Response Policy

Originally Approved: 11-02-10
Approved by: Tom Pelham
Policy Number:

Contents

1.0 Introduction 3

1.1 Authority 3

1.2 Purpose 3

1.3 Scope 3

1.4 Definitions 3

2.0 Policy 4

2.1 General 4

Incident Reporting 4

Escalation 5

Mitigation and Containment 5

Eradication and Restoration 5

Information Dissemination 5

Ongoing Reporting 5

Review 6

2.2 Responsibilities for Physical Security Incidents 6

3.0 Policy Notification 6

1.0 Introduction

1.1 Authority

The Department of Information and Innovation (DII) was created in VSA 22 § 901 (1), "to provide direction and oversight for all activities directly related to information technology, including telecommunications services, information technology equipment, software, accessibility, and networks in state government."

1.2 Purpose

The purpose of this policy is to establish a protocol to guide a response to a computer incident or event impacting State of Vermont computing equipment, data, or networks.

1.3 Scope

For the purpose of this policy, agency/department refers to any State entity including agencies, departments, boards and councils or other entities in the executive branch of government.

This policy applies to all State of Vermont employees, contractors, and others who process, store, transmit, or have access to any state information and computing equipment.

1.4 Definitions

1. **Information Systems:** Any telecommunications and/or computer-related equipment or interconnected system or subsystems of equipment that is used in the acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of voice and/or data (digital or analog): includes software, firmware, and hardware.

2. **Computer Security Incident:** An act or circumstance in which there is a deviation from the requirements of security regulations. Compromise, inadvertent disclosure, need-to-know violation, and administrative deviation are examples of security incidents, including any unauthorized activity that threatens the confidentiality, integrity or availability (CIA) of state information system resources.

3. **Breach:** Vermont's Security Breach Notice Act requires businesses and state agencies to notify consumers in the event a business or state agency suffers a "security breach." A security breach is defined as the "unauthorized acquisition or access of computerized data that compromises the security, confidentiality, or

integrity of personal information maintained by the [business or state agency].” 9 V.S.A. § 2430(8).

4. **Personally identifiable information (PII):** Any piece of information which can potentially be used to uniquely identify, contact, or locate a single person. Data that provides personal or private information that should not be publicly available. For example, PII could be an individual’s Social Security number (SSN), name or address in conjunction with one or more of the following: date of birth, SSN, tax identification number or equivalent, financial account number, and credit or debit card number.

5. **Agency Response Team (ART):** At a minimum, an ad hoc ART assembled to address a breach incident should consist of the department Information Technology (IT) manager(s) experiencing the breach, the Chief Information Officer (CIO), the Security Director, any essential IT and/or physical security staff deemed necessary by the manager or CIO.

2.0 Policy

Incidents are prioritized based on the following:

- Criticality of the affected resources (e.g., public Web server, user workstation)
- Current and potential technical effect of the incident (e.g., root compromise, data destruction).

Combining the criticality of the affected resources and the current and potential technical effect of the incident determines the business impact of the incident—for example, data destruction on a user workstation might result in a minor loss of productivity, whereas root compromise of a public Web server might result in a major loss of revenue, productivity, access to services, and reputation, as well as the release of confidential data (e.g., credit card numbers, Social Security numbers). Refer to the Vermont Functional Classification System at: http://vermont-archives.org/records/vclas/ for more information about classifying data.

2.1 General

Incident Reporting

All computer security incidents, including suspicious events, shall be reported immediately (orally or via e-mail) to the agency/department IT manager and/or department supervisor by the employee who witnessed/identified the breach.

Escalation

The agency/department IT manager and/or department supervisor needs to determine the criticality of the incident (as stated in section 2.0 Policy). If the incident is something that will have serious impact, the department Commissioner and CIO of DII will be notified and briefed on the incident.

The CIO or his/her designee will determine if other agencies, departments, or personnel need to become involved in resolution of the incident. Only the CIO or his/her designee or department Commissioners will speak to the press about an incident.

Mitigation and Containment

Any system, network, or security administrator who observes an intruder on the State of Vermont network or system shall take appropriate action to terminate the intruder's access. (Intruder can mean a hacker, botnet, malware, etc.) Affected systems, such as those infected with malicious code or systems accessed by an intruder shall be isolated from the network until the extent of the damage can be assessed. Any discovered vulnerabilities in the network or system will be rectified by appropriate means as soon as possible.

Eradication and Restoration

The extent of damage must be determined and course of action planned and communicated to the appropriate parties.

Information Dissemination

Any public release of information concerning a computer security incident shall be coordinated through the office of the DII CIO.

The CIO and/or his/her designee shall manage the dissemination of incident information to other participants, such as law enforcement or other incident response agencies. After consulting with the Agency Response Team (ART), he/she shall coordinate dissemination of information that could affect the public, such as web page defacement or situations that disrupt systems or applications.

Ongoing Reporting

After the initial oral or e-mail report is filed, and if the incident has been determined to be a significant event (such as multiple workstations effected, root compromise, data breach, etc.), subsequent reports shall be provided to the CIO and appropriate managers and Commissioners. Incidents such as individual workstations infected with malware are considered minor events and need not be followed up with a written report.

The incident reports shall be submitted within 24 hours of the incident. An agency/department may be required to provide reports sooner in accordance with more stringent regulations. For example: HIPAA, SSA and IRS requirements. If this is the case, the more stringent requirements are to be met.

A general report to the CIO and Security Director of DII shall contain the following:

- Point of contact
- Affected systems and locations
- System description, including hardware, operating system, and application software
- Type of information processed, such as HIPAA related information
- Incident description
- Incident resolution status
- Damage assessment, including any data loss or corruption
- Organizations contacted
- Corrective actions taken
- Lessons learned

A follow-up report shall be submitted upon resolution by those directly involved in addressing the incident.

Review

After the initial reporting and/or notification, the IT manager, department/agency managers and CIO shall review and reassess the level of impact that the incident created.

2.2 Responsibilities for Physical Security Incidents

Refer to Physical Security for Computer Protection Policy at: http://dii.vermont.gov/Policy_Central.

3.0 Policy Notification

Each State agency/department is responsible for ensuring that its employees are aware of where policies are located on websites. Agencies are also responsible for notifying employees of policy change or the creation of new policies that pertain to the agency/department function.