



# DEPARTMENT OF ADMINISTRATION

## Enterprise Policy

DOIT-10-12-2015

### DIVISION OF INFORMATION TECHNOLOGY

#### Information Security Incident Handling and Response

Policy Date of Last Revision 11/10/2015

**Bijay Kumar**

(401) 574-9220

bijay.kumar@doit.ri.gov

#### 1. Purpose

- a. The increasing sophistication and complexity of network attacks pose a considerable threat to the integrity of information system resources. Despite widespread use of firewalls and intrusion prevention and detection hardware and software, information systems continue to be compromised by viruses, malware, social engineering attempts, and unauthorized user activity, whether or not intentional, often resulting in the loss or disclosure of sensitive data. An effective incident response capability is critical for early recognition of security incidents, mitigating loss, and to restore IT services in a timely manner.

#### 2. Purpose

- a. To document an Information Security Incident Handling and Response Policy for the effective and timely management of IT security related incidents in order to safeguard State of Rhode Island IT resources, infrastructure, and data.

#### 3. Scope

- a. This policy covers all State Executive Branch Departments' (including agencies, boards and commissions), and its and their employees, whether permanent, non-permanent, full or part-time, and interns as well as all individuals including, but not limited to, employees, whether permanent, non-permanent, full or part-time, interns, and all consultants, contractors, vendors, contracted individuals, and any entity with access to State data, Confidential Data, or computers and systems operated by the State or maintained on behalf of the State.

#### 4. Authority

- a. Executive Order 04-06 established the Division of Information Technology ("DoIT") within the Department of Administration to improve the efficiency, effectiveness, and security of IT management and operations within the Executive Branch of the State of Rhode Island. In accordance with Executive Order 04-06, DoIT will define, maintain, and enforce statewide IT related policies and procedures for the effective use and security of IT resources.

#### 5. Definitions and Acronyms

- a. **AIM** - Agency Information Manager
- b. **DoIT Chief** - The individual acting as the head of DoIT as determined by the Director of Administration.

- c. **Computer Incident Response Team (CIRT)** - A team of knowledgeable and skilled individuals tasked with responding to and resolving security incidents in order to limit their scope, magnitude, and impact to IT systems and data.
  - d. **CISO** - DoIT Chief Information Security Officer
  - e. **Confidential Data** - Data that is PIT, PHI, SSI, FTI or required by law, regulation or policy to be kept confidential.
  - f. **DoIT** - Division of Information Technology
  - g. **EISO** - DoIT Enterprise Information Security Office
  - h. **Enterprise CIRT** - The Computer Incident Response Team appointed by the DoIT Chief.
  - i. **FTI** - Federal Tax Information
  - j. **HIPAA** - Health Insurance Portability and Accountability Act, Health Insurance Technology for Economic and Clinical Health Act, plus their amendments, regulations and policies.
  - k. **IT** - Information Technology
  - l. **NNSC**- National Network Service Center
  - m. **PCI** - Payment Card Industry
  - n. **PHI** - Protected Health Information (HIPAA)
  - o. **PII** - Personally Identifiable Information
  - p. **SSA** - Social Security Administration
  - q. **SSI** - Social Security Information
  - r. **SSN**- Social Security Number
  - s. **Security Incident** - An actual or perceived event arising from a risk, threat, or vulnerability that may affect the confidentiality, integrity, or availability of information resources or data, cause damage to IT systems and/or network, or result in a significant loss of vital business assets.
  - t. **TSM** - Technical Support Manager
  - u. **US-CIRT** - United States Computer Incident Response Team
6. **Policy**
- a. **Incident Response Training.** Information system users will be periodically trained in accordance with assigned incident handling and response roles and responsibilities.
  - b. **Incident Response Testing.**
    - (i.) Incident handling and response capabilities will be periodically tested to assess the effectiveness of incident response.
    - (ii.) Incident handling and response test results will be documented and reviewed.

- (iii.) Federal Tax Information (FTI). Agencies that handle or process FTI will, in coordination with DoIT:
  1. Create security incident scenarios that test for breaches of FTI.
  2. Include all Agency personnel or contractors assigned incident handling and response roles and responsibilities in breach of FTI tests.
  3. Perform post-test reviews to improve existing processes and procedures.

**c. Incident Handling**

- (i.) The incident handling and response capability will include the following steps:
  1. *Preparation*: Establish processes, procedures, and guidance for the incident handling and response capability.
  2. *Detection and Analysis*: Assess and categorize security incidents.
  3. *Containment*: Limit the scope, magnitude, and impact of the security incident.
  4. *Notification*: Notify appropriate parties.
  5. *Eradication*: Remove the cause of the incident and mitigate the vulnerabilities.
  6. *Recovery*: Return systems and business processes to normal operational status.
- (ii.) Incident handling and response activities will be included in and coordinated with disaster recovery and contingency planning activities.
- (iii.) Lessons learned from incident handling and response activities will be documented and incorporated into incident handling and response procedures, training, and testing.
- (iv.) An Enterprise CIRT will be established by the DoIT Chief for handling and responding to security incidents whose scope impacts the Enterprise network and/or infrastructure and security incidents involving the unauthorized access and/or release of Confidential Data. The Agency will establish a CIRT that will include the AIM and TSM for handling and responding to security incidents whose scope is restricted to the Agency and does not involve the unauthorized access and/or release of Confidential Data. The Agency CIRT will assist the Enterprise CIRT as directed.

**d. Incident Monitoring.** Security incidents will be monitored and tracked to closure on an ongoing basis.

**e. Incident Reporting.** Actual or suspected security incidents will be reported to appropriate authorities in a timely manner and in accordance with all applicable laws, regulations, and policies. If time permits, Legal will be notified of any actual or suspected security incidents prior to reporting to appropriate authorities.

**f. Incident Response Assistance.** The Service Desk will provide information system users with assistance and advice for handling and reporting security incidents.

**g. Incident Response Plan.**

- (i.) An incident response plan will be developed and disseminated to appropriate Agency personnel that provides guidance for, describes the structure of, and defines the metrics, resources, and management support required to maintain an effective incident handling and response capability.
- (ii.) The Agency will develop incident handling and response procedures that address its unique business processes. These procedures will not supersede established DoIT policy, but may be more stringent.
- (iii.) The incident response plan will be reviewed annually and updated as required.
- h. Policy Reviews.** This Policy will be reviewed annually and updated as required.
- i. Noncompliance.** Any employee, person or entity that violates this Policy may be subject to disciplinary action up to and including termination.
- j. Waivers.** The Agency may request a waiver from this Policy by formally submitting justification for the waiver and demonstrating that compensating controls are in place to mitigate the risk. If approved, the Agency Director must accept in writing all risk to IT system resources and data associated with the waiver. Waivers require approval from and are granted solely by the DoIT Chief. Waivers expire one year from date of issue, or upon the ending for the reason of the waiver, whichever occurs sooner. The Do IT Chief shall have the authority to renew or rescind any waiver granted pursuant to this section.
- k. Standards and Procedures.** The CISO and Do IT Chief may approve and adopt Standards and/or Procedures to effectuate the purpose of this Policy. Any Procedures adopted pursuant to this section should be fluid in nature to allow for timely adjustments and improvements.
- l. Amendment.** This Policy, its Standards and Procedures may be amended or rescinded at any time without further notice.

## 7. Roles and Responsibilities

### a. *Chief Information Security Officer*

- (i.) Periodically review and update policy, as required.
- (ii.) Develop, disseminate, and periodically review the incident response plan.
- (iii.) Ensure compliance with and enforce policy provisions.
- (iv.) Member of Enterprise CIRT.
- (v.) Monitor and track security incidents.

### b. *Agency*

- (i.) Comply with policy provisions.
- (ii.) Develop incident response procedures that address its unique business processes.
- (iii.) Establish an Agency CIRT.
- (iv.) Assist Enterprise Information Security Office in monitoring and tracking security incidents.

**8. Assistance**

Service Desk

ent.servicedesk@ri.gov

401.462-4357

**9. Signatures**



Chief Digital Officer, Office of Digital Excellence /  
Head of the Division of Information Technology

11/10/15

Date



Chief Information Security Officer,  
Division of Information Technology

4/13/05

Date



Director, Department of Administration

11/10/15

Date