Enterprise Technology Strategy and Services Policy 10-12

Incident Handling and Response (IR)  
Brian Tardiff, CISO  
Last Revision: 3/1/2021  
doa.entsec@doit.ri.gov

1. Purpose

Establish policy for the effective and timely management of IT security related incidents to safeguard State of Rhode Island IT resources, infrastructure, and data. Maintain an effective incident response capability that identifies early recognition of events and security incidents, mitigates loss, and restores IT services and network resources in a timely manner.

2. Applicability

This policy is applicable to all State of Rhode Island Executive Branch Departments\(^1\) (including agencies, boards and commissions), and their employees (including permanent, non-permanent, full-time, and part-time) and interns, consultants, contractors, vendors, contracted individuals, and any entity having access to state information systems and data, whether operated or maintained by the state or on behalf of the state. For this policy, the term "agency" is used to refer to any department, agency, division, or unit of the Executive branch of the State of Rhode Island.

3. Definitions

**Incident Response Team (IRT)**
A team of knowledgeable and skilled individuals tasked with responding to and resolving security incidents to limit their scope, magnitude, and impact to IT systems and data. In accordance with the DoIT Incident Handling and Response Plan (Guideline 10-12G), there are two (2) IRTs: an agency IRT and an EOC IRT.

**Information Spillage**
An instance where sensitive information is inadvertently placed on an information system that is not authorized to process such information.

**Federal Tax Information (FTI)**
Federal tax returns and return information (and information derived from it) in the state agency’s possession or control covered by confidentiality protections of the Internal Revenue Code (IRC) and subject to IRC 6103(p)(4) safeguarding requirements, including Internal Revenue Service (IRS) oversight. FTI includes return or return information received directly from IRS or obtained through an authorized secondary source, such as Social Security

---

\(^1\) State of Rhode Island Executive Branch Departments does not include the University of Rhode Island, the State Colleges, the General Treasurer, the Attorney General, or the Secretary of State.
Administration (SSA), Federal Office of Child Support Enforcement (OCSE), Bureau of the Fiscal Service (BFS), or Centers for Medicare and Medicaid Services (CMS), or other entity acting on behalf of the IRS pursuant to an IRC 6103(p)(2)(B) Agreement. FTI includes any information created by the recipient that is derived from federal return or return information received from IRS or obtained through a secondary source. Safeguarding FTI is critical to protecting taxpayer confidentiality as required by IRC 6103 and may not be masked to change the character of information to circumvent IRC 6103 confidentiality requirements.

National Directory of New Hires (NDNH) Data
A national database of wage and employment information operated by the federal Office of Child Support Enforcement (OCSE) and used to assist states administering programs that improve states’ abilities to locate parents, establish paternity, and collect child support. The NDNH is located at the Social Security Administration’s (SSA) National Support Center. The NDNH database contains new hire, quarterly wage, and unemployment insurance information and is only available to authorized persons or entities for authorized purposes. NDNH data includes:
• Employee name, address, data of hire, wage, reporting period, and SSN
• Employer name, address, and Federal Employer Identification Number (FEIN)
• Claimant name, address, benefit amount, reporting period, and SSN

Security Event
An observable event arising from a risk, threat, or vulnerability that may impact the confidentiality, integrity, or availability of state network resources, information system damage, network disruption, or significant loss of vital business assets.

Security Incident
A security event that results in a compromise to the confidentiality, integrity, or availability of state network resources, including information system damage, network disruptions, or significant loss of vital business assets. A security event that results in the unauthorized disclosure of confidential data is also known as a security breach.

Social Security Administration (SSA) Data
Data under the control of SSA provided to the state agency under the terms of an Information Exchange Agreement with the SSA, including data provided to the state agency by a source other than SSA but for which the state agency attests to that the SSA verified it or the state agency couples the data with other SSA data to certify its accuracy. SSA data includes:
• SSA’s response to a request from the state agency for information from SSA (e.g. date of death).
• SSA’s response to a query from the state agency for verification of an SSN.
• Display by the state agency of SSA’s response to a query for verification of an SSN and the associated SSN provided by SSA.
• Display by the state agency of SSA’s response to a query for verification of an SSN and the associated SSN provided to the state agency by a source other than SSA.
• Electronic records that contain only SSA’s response to a query for verification of an SSN and the associated SSN whether provided to the state agency by SSA or a source other than SSA.

4. Procedures for Compliance

Security controls in this policy will be implemented in accordance with the security categorization of the information system. The security categorization is based on the Information Assurance Level (IAL) requirements of the information system.

<table>
<thead>
<tr>
<th>Low Risk Systems (IAL1)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information systems that only contain data that is public by law or directly available to the public via mechanisms such as the internet. In addition, desktops, laptops, and supporting systems used by agencies are Low Risk unless they store, process, transfer, or communicate private or sensitive data.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Moderate Risk Systems (IAL2)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information systems that store, process, transfer, or communicate private or sensitive data or have a direct dependency on a Moderate system. At a minimum, any information system that stores, processes, transfers, or communicates PII or other sensitive data types is classified as a Moderate system.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.1. [IAL1, IAL2] Incident Response Policy and Procedures (IR-1).</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agency will develop, document, disseminate, review, and annually update an incident response policy and procedures. Incident response policy and procedures will be disseminated to designated personnel defined in the applicable system security plan, agency information managers (AIM), technical support managers (TSM), data owners, system owners, system administrators, and any other personnel or roles the agency determines require access.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.2. [IAL1, IAL2] Incident Response Training (IR-2).</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agency will provide incident response training to information system users consistent with their assigned roles and responsibilities within three (3) months of assigning the incident response role or responsibility to the user, when required after an information system change, and annually thereafter. IRT team members will be periodically trained regarding key aspects of their incident handling and response responsibilities. The agency will maintain a training log that includes the training participant name, training date, and training type and description.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>4.3. IAL2/ Incident Response Testing (IR-3).</th>
</tr>
</thead>
<tbody>
<tr>
<td>The agency will perform annual incident response testing to assess the agency incident response capability, and document and review incident response test results. The agency will document an after-action report</td>
</tr>
</tbody>
</table>
from incident response testing to improve current processes and procedures and incorporate lessons learned into future incident response training and testing exercises. Agencies that handle FTI will perform annual tabletop incident response exercises using breach of FTI scenarios that includes all employees and contractors with incident response responsibilities. Formal incident response testing is not required if the agency actively implements and exercises its response capability for an actual incident during the calendar year.

4.3.1. [IAL2] Coordination with Related Plans (IR-3.2). The agency will coordinate incident response testing with personnel responsible for other risk management activities, including, as appropriate, business continuity, disaster recovery, continuity of operations, and critical infrastructure planning.

4.4. [IAL1, IAL2] Incident Handling (IR-4). The agency will (i) implement an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery activities, (ii) coordinate incident handling activities with contingency planning activities, (iii) preserves evidence through a technical means, including secured storage of evidence media, "write" protection of evidence media, sound forensics processes and utilities that support legal requirements, and follows a chain of custody for forensic evidence, and (iv) incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing exercises. See DoIT Incident Handling and Response Plan for more information.

4.4.1. [IAL2] Automated Incident Handling Processes (IR-4.1). The agency will use automated mechanisms to support the incident handling process (e.g. ServiceNow Incident Management Portal).

4.5. [IAL1, IAL2] Incident Monitoring (IR-5). The agency will monitor and document information system security incidents to closure.

4.6. [IAL1, IAL2] Incident Reporting (IR-6). The agency will require personnel who observe a possible security incident to, in accordance with local emergency procedures, immediately notify the local Damage Assessment Team (DAT), building security personnel, and/or other designated personnel of the incident in accordance with procedures documented in the DoIT Incident Handling and Response Plan.

FTI Data Breach Reporting Procedure
If the agency experiences or suspects a breach or loss of PII or security incident that involves FTI, including unauthorized disclosure or access to FTI, the agency will immediately, but no later than 24 hours after identifying a possible issue involving FTI, notify the ETSS CISO, contact the special agent-in-charge, contact the Treasury Inspector General for Tax Administration (TIGTA) of the New York field office at (917)-408-5640, and email the IRS Office of Safeguards at safeguardreports@irs.gov. If unable to contact the local TIGTA office, please contact the hotline number at 1-900-589-3718. Immediate notification to the IRS Office of Safeguards is the most important factor, not
the completeness of the data incident report. Send the data incident report electronically and encrypted via an IRS-approved encryption technique. Use the term “Data Incident Report” in the subject line of the email. When emailing the Office of Safeguards, please include the following information in the data incident report (do not include any FTI):

- Name of agency and agency point of contact.
- Date and time incident occurred.
- Date and time incident were discovered.
- How incident was discovered.
- Description of incident and data involved, including specific data elements (if known).
- Physical address where incident occurred and IT equipment involved (e.g. laptop, server, mainframe).

SSA Data Breach Reporting Procedure
If the agency experiences or suspects a breach or loss of PII or security incident which includes SSA data, the ETSS CISO and agency official designated in the IEA as the individual responsible for systems security will be immediately notified. If, for any reason, the agency official is unable to make contact with the SSA Regional Office or SSA Systems Security Contact within one (1) hour, the agency official will report the incident by calling the SSA’s National Network Service Center (NNSC) toll free at 1-877-697-4889 on behalf of the Data Exchange Coordinator (DEC) for his/her region (select “Security and PII Reporting” from the options list). As the final option, in the event SSA contacts and NNSC both cannot be reached, the agency will contact SSA’s Office of Information Security, Security Operations Center at 1-866-718-6425. The agency will provide the SSA contact with timely updates as they become available. The agency should refer to the worksheet provided in the IEA to facilitate the gathering and organizing of information about the incident. The current SSA Project Coordinator & Regional Office Contact is:

Susan Fay, Data Exchange Coordinator
Social Security Administration
Center for Programs Support
JFK Federal Building, Room 1925
Boston, MA 02203
Phone: 1-617-565-2855
Fax: 1-617-565-9359
Email: Susan.Fay@ssa.gov and BO.MA.RO.CPS.Data.Exchange@ssa.gov

NDNH Data Breach Reporting Procedure
If the state agency experiences a confirmed or suspected loss of personal information or a security incident that involves NDNH data, the state agency will immediately, but no later than one (1) hour after the discovery of the incident, notify, in electronic or physical form, the agency security point of contact, the ETSS CISO, and Federal Parent Locator Service (FPLS) Information Systems Security Officer (ISSO). The current FPLS contact Linda Boyer (linda.boyer@acf.hhs.gov), Associate Commissioner of the Office of Child Support Enforcement, who may be reached at 1-202-401-5410 (fax number 1-202-401-5553). When contacting the FPLS, please provide the following information:
Name of agency and agency security point of contact.
Date and time incident occurred.
Date and time incident was discovered.
How incident was discovered.
Description of incident and data involved, including specific data elements (if known).
Address where incident occurred and IT equipment involved (e.g. laptop, server, mainframe).

4.6.1. [IAL2] Automated Reporting (IR-6.1). The agency will use automated mechanisms to assist in the reporting of security incidents (e.g. Enterprise Service Desk).

4.7. [IAL1, IAL2] Incident Response Assistance (IR-7). The agency will provide an incident response support resource, integral to the agency incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents. For general incident response assistance, please contact ETSS Enterprise Service Desk at (401) 462-4357 or ent.servicedesk@ri.gov.

4.7.1. [IAL2] Automation Support for Availability of Information/Support (IR-7.1). The agency will use the ETSS ServiceNow Incident Management Portal and, where required, other automated mechanisms to increase response-related information and support.

4.8. [IAL1, IAL2] Incident Response Plan (IR-8). ETSS has developed an Incident Response Plan (IRP) that:
1. Provides a roadmap for implementing the incident response capability.
2. Describes the structure of the incident response capability.
3. Provides a high-level approach for how the incident response capability fits aligns with Enterprise risk management strategy.
4. Meets the unique mission, size, structure, and functional requirements of the agency and Enterprise.
5. Defines reportable incidents.
6. Provides metrics for measuring the incident response capability at the agency.
7. Defines resources and management support necessary to maintain an effective incident response capability.
8. Addresses the sharing of incident information.
9. Explicitly designates responsibility for incident response to designated Enterprise and agency personnel.
10. Is reviewed annually by the IRP owner (Chief Digital Officer) and updated, as required, to address changes to information systems or organizational personnel, or due to issues encountered during plan implementation, execution, or testing.

The agency will:
1. Distribute the IRP to authorized incident response personnel defined in the IRP.
2. Protects the IRP from unauthorized modification or disclosure.
3. Within 30 days of a change being made, communicate IRP changes to authorized incident response personnel.

4. Immediately activate the IRP for any of the following events:
   a. Statewide service outage.
   b. Agency service outage impacting agency customers.
   c. Service outage impacting a single department or location.
   d. Actual or suspected cyber event (e.g. malware, denial of service).
   e. Loss or breach of data categorized above public.
   f. Critical service impacting twenty-five (25) or more users.
   g. Emergency request from the Governor’s office

5. Approval / Review Signature

   [Signature]

   Digitally signed by Brian Tardiff
   Date: 2021.10.25 12:29:22
   -04'00'

   Chief Information Security Officer