Division of Enterprise Technology Strategy and Services

ETSS Policy 300.8

Cybersecurity Incident Handling and Response Policy (IR)

Publish Date: 23 July 2026
Effective Date: 23 July 2026
Last Review: 22 July 2026

doa.entsec@doit.ri.gov

1. Purpose

This policy establishes the requirements for the effective and timely management of cybersecurity incidents to safeguard State of Rhode Island information systems, infrastructure, and data. It defines an incident response capability that supports early recognition of events and cybersecurity incidents, rapid containment and mitigation of loss, timely restoration of IT services and network resources, preservation of forensic evidence, and compliance with federal and State breach notification requirements. The incident response lifecycle encompasses preparation, detection and analysis, containment, eradication, recovery, and post-incident activities.

This policy supports the State's compliance with NIST SP 800-53 Revision 5 (Incident Response family), NIST SP 800-61 (Computer Security Incident Handling Guide), NIST Cybersecurity Framework 2.0, IRS Publication 1075, and other applicable federal and state regulatory requirements, as well as the ETSS Major Incident Response Plan.

2. Applicability

This policy applies to all State of Rhode Island Executive Branch departments, including agencies, boards, and commissions, as well as their employees (permanent, non-permanent, full-time, and part-time), interns, consultants, contractors, vendors, and any entity that has access to State information systems and data, whether operated or maintained by the State or on behalf of the State.

3. Roles and Responsibilities

3.1. Chief Information Security Officer (CISO)

Designated by the Chief Digital Officer as the official responsible for the enterprise Incident Response policy and as the Primary Incident Handler. Oversees the enterprise cybersecurity incident response capability, leads unified command activation for critical breach events, coordinates federal breach notifications (FTI, SSA, NDNH), directs forensic investigations, and provides post-incident analysis and lessons learned.

3.2. Chief Digital Officer (CDO)

Owner of the Incident Response Plan (IRP). Reviews and approves the IRP annually in conjunction with the CISO and CTO. Provides executive oversight for incidents with

enterprise-wide impact.

3.3. Chief Technology Officer (CTO)

Reviews and approves the IRP annually. Coordinates infrastructure recovery and restoration activities during and after incidents. Provides technical escalation support for complex infrastructure-related incidents.

3.4. ETSS Security Operations

Serves as the primary coordination point for cybersecurity incident response. Operates enterprise SIEM (Microsoft Sentinel) and EDR (CrowdStrike Falcon) platforms for detection and analysis. Executes containment, eradication, and recovery actions. Monitors and tracks cybersecurity incidents to closure through ServiceNow.

3.5. System Owners

Responsible for implementing incident handling capabilities for their systems, coordinating with ETSS to develop on system-specific response procedures, providing technical expertise during incident investigations, and ensuring post-incident corrective actions are completed.

3.6. Agency Information Managers (AIMs) / Technical Support Managers (TSMs)

Coordinate incident response activities at the agency level. Serve as the primary agency liaison with ETSS Security Operations during incidents. Ensure agency personnel are trained in incident reporting procedures.

3.7. All Personnel

Responsible for immediately reporting any observed or suspected cybersecurity incident to the ETSS Enterprise Service Desk. Must not attempt to investigate, contain, or remediate incidents independently without authorization from the ETSS Security Operations team.

4. Procedures for Compliance

The following requirements establish the incident response controls that agencies and ETSS must implement.

4.1 Incident Response Policy and Procedures (IR-1)

Applies to: All systems (IAL1, IAL2)

Each agency shall adopt this policy and develop, document, and disseminate supporting procedures. The ETSS CISO is designated as the official responsible for the enterprise policy and is the designated Cybersecurity Incident Handler. The policy shall be reviewed at least every three (3) years and following significant changes. Supporting procedures shall be reviewed annually.

4.2 Incident Response Training (IR-2)

Applies to: All systems (IAL1, IAL2)

ETSS shall:

a. Provide incident response training to personnel consistent with their assigned roles and responsibilities within thirty (30) days of assignment, when required after a system change, and annually thereafter. Training may be included as part of annual cybersecurity awareness training. A training log shall be maintained with participant names, training dates, and training names.

b. Review and update incident response training content every three (3) years, after an unauthorized disclosure of classified information, and following a cybersecurity incident that impacts three or more agencies. For agencies handling FTI, annual tabletop exercises using FTI breach scenarios are required and must include all personnel with incident response responsibilities.

4.3 Incident Response Testing (IR-3)

Applies to: Moderate and above (IAL2)

ETSS shall:

a. Perform annual incident response testing to assess the agency's incident response capability. Testing is not required if the agency actively implements and exercises its response capability for an actual major incident during the calendar year. Testing methods include checklists, walk-throughs, tabletop exercises, simulations, and comprehensive tests, selected based on the criticality and IAL of the information system.

b. Document an after-action report from testing to improve current processes and incorporate lessons learned into future training and testing exercises.

4.3.1 Coordination with Related Plans (IR-3(2))

Applies to: Moderate and above (IAL2)

ETSS shall coordinate incident response testing with personnel responsible for related plans, including business continuity, disaster recovery, continuity of operations, and critical infrastructure planning.

4.4 Incident Handling (IR-4)

Applies to: All systems (IAL1, IAL2)

ETSS shall:

a. Implement an incident handling capability for cybersecurity incidents that includes preparation, detection, analysis, containment, eradication, recovery, and post-incident activities in accordance with the ETSS Incident Response Plan. Evidence shall be preserved through technical means, including secured storage of evidence media, write-protection, sound forensic processes, and chain of custody for forensic evidence.

b. Coordinate incident handling activities with contingency planning activities. Incident handling shall be coordinated across ETSS Security Operations, TSMs, AIMs, system owners, and agency leadership, with escalation to legal counsel, privacy officials, communications, human resources, law enforcement, or regulatory authorities as applicable.

c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing exercises. All incidents shall be documented and tracked from initial detection through closure using enterprise service management and incident tracking mechanisms.

4.4.1 Automated Incident Handling Processes (IR-4(1))

Applies to: Moderate and above (IAL2)

Each agency shall use ETSS authorized automated mechanisms to support the incident handling process, including enterprise SIEM systems (Microsoft Sentinel), endpoint detection and response platforms (CrowdStrike Falcon), network

monitoring systems, and the ServiceNow Incident Management Portal.

4.5 Incident Monitoring (IR-5)

Applies to: All systems (IAL1, IAL2)

ETSS shall monitor, track, and document cybersecurity incidents to closure.

4.6 Incident Reporting (IR-6)

Applies to: All systems (IAL1, IAL2)

Each agency shall require personnel who observe a possible cybersecurity incident to immediately notify the ETSS Enterprise Service Desk (ent.servicedesk@ri.gov or 401-462-4357) and appropriate IRT personnel in accordance with the ETSS Incident Response Plan. For actual or suspected breaches involving FTI, SSA, or NDNH data, the following reporting procedures apply:

FTI Data Breach Reporting: If the agency experiences or suspects a breach involving FTI, the agency shall immediately, but no later than 24 hours after identification, notify the ETSS CISO, contact the IRS special agent-in-charge, and email the IRS Office of Safeguards at safeguardreports@irs.gov. The data incident report shall be sent encrypted using an IRS-approved encryption method with the subject line "Data Incident Report" and shall include: agency name and point of contact, date and time of incident occurrence and discovery, how the incident was discovered, description of the incident and data involved, potential number of FTI records involved, physical address and IT equipment involved, and whether the incident involves an agency employee.

SSA Data Breach Reporting: If the agency experiences or suspects of a breach involving SSA data, the ETSS CISO and the agency representative designated in the Information Exchange Agreement shall be immediately notified. If the agency is unable to contact the SSA Regional Office or SSA Systems Security Contact within one (1) hour, the agency shall call SSA's National Network Service Center toll-free at 1-877-697-4889.

NDNH Data Breach Reporting: If the agency experiences or suspects a breach involving NDNH data, the agency shall immediately, but no later than one (1) hour after discovery, notify the agency security point of contact, the ETSS CISO, and the Federal Parent Locator Service (FPLS) Information Systems Security Officer.

4.6.1 Automated Reporting (IR-6(1))

Applies to: Moderate and above (IAL2)

ETSS shall use automated mechanisms to assist in reporting critical cybersecurity incidents, including statewide or agency service outages, actual or suspected cyber events, breach or loss of classified data, critical services impacting twenty-five or more users, and emergency requests from the Governor's Office.

4.6.2 Supply Chain Coordination (IR-6(3))

Applies to: Moderate and above (IAL2)

ETSS shall provide incident information, as required, to supply chain providers for information systems or system components related to the incident. Information shared with supply chain partners shall be limited to what is necessary for investigation and remediation and reviewed for legal, privacy, and contractual considerations prior to release.

4.7 Incident Response Assistance (IR-7)

Applies to: All systems (IAL1, IAL2)

Each agency shall identify an incident response support resource that offers advice and assistance to users for the handling and reporting of cybersecurity incidents. ETSS Security Operations serves as the primary coordination point for enterprise incident response assistance. For general assistance, contact the ETSS Enterprise Service Desk at ent.servicedesk@ri.gov or 401-462-4357.

4.7.1 Automation Support for Availability of Information and Support (IR-7(1))

Applies to: Moderate and above (IAL2)

Each agency shall use ETSS authorized automated mechanisms to increase the availability of incident response information and support, including the ServiceNow Incident Management Portal and enterprise major incident email communications.

4.8 Incident Response Plan (IR-8)

Applies to: All systems (IAL1, IAL2)

ETSS has developed and maintains a formal Incident Response Plan (IRP) that provides a roadmap for implementing the incident response capability, describes the structure of the response capability, aligns with the enterprise risk management strategy, defines reportable incidents, provides metrics for measuring response capability, defines resources and management support, addresses sharing of incident information, and explicitly designates responsibility for incident response. The IRP shall be reviewed and approved by the CDO, CISO, and CTO at least annually.

Each agency, with ETSS support shall:

a. Develop agency-specific incident response and business continuity procedures as necessary to address agency-specific business processes.

b. Distribute the IRP to authorized incident response personnel and communicate changes within 30 days.

c. Protect the IRP from unauthorized disclosure or modification.

d. Immediately activate the IRP for any of the following events: statewide service outage, agency service outage impacting customers, service outage impacting a single department or location, actual or suspected cyber event (such as malware or denial of service), loss or breach of classified data, critical service impacting twenty-five or more users, or emergency request from the Governor's Office.

4.9 Information Spillage Response (IR-9)

Applies to: Moderate and above (IAL2)

Each agency shall respond to information spillage (the inadvertent placement of classified information on systems not authorized to process such information) by: identifying the specific information involved, alerting the ETSS CISO and designated personnel, isolating the contaminated system or component, securely eradicating the spilled information using approved methods, identifying other systems that may have been subsequently contaminated, and following established response playbooks and procedures.

4.9.1 Information Spillage Training (IR-9(2))

Applies to: Moderate and above (IAL2)

ETSS shall provide information spillage response training at least annually to designated personnel with incident response responsibilities. Changes to the IRP

regarding data spillage shall be summarized for stakeholders and included in annual training.

4.9.2 Post-Spill Operations (IR-9(3))

Applies to: Moderate and above (IAL2)

Each agency shall implement procedures to ensure that personnel impacted by information spillage events can continue to carry out assigned tasks while contaminated systems undergo corrective actions, including root cause analysis and identification of contributing factors.

4.9.3 Exposure to Unauthorized Personnel (IR-9(4))

Applies to: Moderate and above (IAL2)

Each agency shall employ procedures for personnel exposed to information not within their authorized access, including notification, documentation, and any additional security measures required to mitigate the exposure.

5. Approval / Review Signatures

Digitally signed by Nathan Loura
Date: 2026.07.29 12:34:13 -04'00'

Chief Information Security Officer (CISO)
Division of Enterprise Technology Strategy and Services

Brian Tardiff
Digitally signed by Brian Tardiff
Date: 2026.07.29 13:52:10 -04'00'

Chief Digital Officer (CDO)
Division of Enterprise Technology Strategy and Services