Cyber Security Incident Response Plan Procedure

Section/Group

Security

Purpose

This procedure defines the Cyber Security Incident Response Plan.

Scope

This procedure applies to all DTS employees.

Term

To be reviewed annually.

Procedure

Document History

Original Submission

Issue Date: 10/15/2015
Effective Date: 10/15/2015

Revisions

Last Revised Date: 08/21/2025

Reviews

Next Review: 05/05/2026

Procedure

Incident Prevention

The Division of Technology Services (DTS) has the responsibility to provide anti-malware protection on all network infrastructure devices, servers, and end user computing devices as indicated:

- The Enterprise Information Security Office (EISO) manages an enterprise anti-malware solution to facilitate this security objective. To meet this objective:
- For all end user devices, the EISO utilizes endpoint protection
- For all servers, EnterpriseDevOps support is required to implement and manage malware protection solutions.
- For all network infrastructure devices, Network operations is required to implement and manage malware protection solutions
- The EISO is responsible for auditing all devices for compliance with this objective. The EISO currently performs vulnerability assessments and penetration tests on a quarterly basis to ensure that compliance with this objective is maintained.
- The EISO is responsible for 24/7 continuous monitoring to detect and mitigate malware related security events.
- The EISO audits all system configurations annually and provides continuous monitoring of configuration and system access changes via the Enterprise SIEM solution

Incident Response Planning

The Cyber Security Incident Response Plan (CSIRP) provides guidance and documentation on cyber security incident response handling and communication efforts. The CSIRP is activated whenever a computer-related security incident occurs, and guides the responses to all incidents whose severity is such that they could affect the State’s ability to do business, or undermine its reputation. When a security incident occurs, reactions and decisions must be made very quickly (often in a matter of minutes). The State of Utah has to be prepared to deal with these incidents as soon as they occur; waiting until a new product arrives or a consulting engagement is completed is not an option. Incident response planning is a functional requirement managed by the Enterprise Information Security Office (EISO), and directed by the Chief Information Security Officer (CISO).

- The CISO will conduct an incident response planning meeting annually. The purpose of the incident response planning is to review and update the CSIRP.
- The EISO will conduct incident response training, involving the Cyber Security Incident Response Team (CSIRT) quarterly. The purpose of the required training is to practice various scenarios involving the identification of a computer related security incident, notification of the Cyber Security Incident Response Team, and a defined response methodology.
- The EISO will establish metrics for incident response management as defined in this plan. The established metrics will be reviewed by DTS executive management annually.

Incident Response Training

Users who have an incident response role or responsibility will be trained on a yearly basis to ensure they understand their roles and responsibilities as it pertains to incident response.

What is an Incident

An Incident is defined as an act in violation of legal statute, or in violation of the explicit or implied security policies of the organization, with or without intent to do harm. The types of activity considered to be in violation of the Utah Department of Technology Services (DTS) Enterprise Information Security Policy are characterized below. These activities include but are not limited to:

- A system resource is exposed or is potentially exposed to unauthorized access.
- Legitimate and authorized access to an information system or service is interrupted or denied.
- Any adverse event which compromises the authentication and access to a software application, computer system, or network.
- The unauthorized use of a system for the processing or storage of data.
- The unauthorized alteration of data transferred and stored electronically.
- Changes to system hardware, firmware, or software characteristics without the owner’s knowledge, instruction or consent.

Incident Detection

Incident detection is facilitated through 24/7 continuous threat monitoring by Division of Technology Services trained security analysts and multiple tools, including Security Information and Event Management SIEM, Intrusion Prevention Systems (IPS), Intrusion Detection Systems (IDS), Vulnerability Scanning and Management, Anti-Virus Detection and Removal, and Threat Monitoring Services. Trained staff monitors multiple systems and responds to technical anomalies and automated alerts. Automated alerts are generated through the SIEM system and distributed via email and SMS messaging to authorized staff and management personnel.

Additional processes are implemented to promote security awareness and the reporting of known or suspicious activity related to a security incident. The symptoms of an incident could be the sudden degradation in server or network performance, asset compromise, failure of service(s), defacement of website contents, spam email, mail route abuse, etc. Established metrics used to track incident detection include the following:

- The EISO manages a SIEM product used to monitor logs from network devices such as firewalls and routers, Intrusion Detection Systems (IDS), and servers. Metrics related to security events are reported to DTS and agency management from the SIEM product to a web based dashboard on a daily basis. The EISO utilizes the SIEM product to actively monitor threat and security events in real time 24/7/365. The SIEM provides real-time threshold alarms and notifications to appropriate security, technical support, and agency personnel.
- The EISO actively monitors the enterprise network for incident detection and submits work order tickets to appropriate technical support groups including the network operations center, enterprise DevOps, Edge support, and law enforcement entities.
- The EISO continuously updates and manages threshold alarms in the SIEM. Security Analysts tasked with threat monitoring receive alarm notifications in near real time for review and mitigation as defined in this CSIRP.

Incident Reporting

A suspected incident with a severity of 4 or 5, as indicated below should immediately be reported to the Enterprise Information Security Office (EISO). Notification can be made using any of the following methods:

- E-mail to DTS-SOC@utah.gov
- SOC 24×7 Phone – (801) 538-3011
- Helpdesk notification
- On-line Security Notification form – ServiceNow > Service Catalog > Security Forms > Security Incident Notification

All suspected incidents at any severity level should be reported to DTS-Enterprise Security using any of the above described methods.

The initial incident report should include all IP addresses and/or evidence available at the time of the incident detection.

Incident Severity and Declaration

Many security incidents, such as isolated occurrences of computer viruses, are efficiently managed using deployed processes and procedures without activating the CSIRP and notifying the entire Cyber Security Incident Response Team (CSIRT). The following criteria will be used to classify the severity of security incidents, and which severities will result in CSIRP activation.

Incident Severity:

Severity 1 (Minor Incident) – Small numbers of system probes or scans detected on internal systems; isolated instances of known computer viruses handled by antivirus software.

Severity 2 (Elevated Incident) – Small numbers of system probes or scans detected on external systems; intelligence received concerning threats to which systems may be vulnerable.

Severity 3 (Moderate Incident) – Significant numbers of system probes or scans detected; penetration or denial of service attacks attempted with no impact on operations; widespread instances of known computer viruses handled by anti-virus software; isolated instances of a new computer virus not handled by anti-virus software.

Severity 4 (Major Incident) – Penetration or denial of service attacks attempted with limited impact on operations; widespread instances of a new computer virus not handled by anti-virus software; some risk of negative financial or public relations impact.

Severity 5 (Critical Incident) – Successful penetration or denial of service attacks detected with significant impact on operations; significant risk of negative financial or public relations impact.

Incidents of Severity 4, or 5 will result in CSIRP activation, while incidents of Severity 1, 2, or 3 will be handled without CSIRT involvement.

Incident Declaration, Reporting and Notification

When an incident requiring CSIRP activation occurs, a formal incident declaration will be made by the CISO or authorized delegate. The CISO is responsible to notify CSIRT members, upper-level management in DTS, and pre-defined contacts in the affected organizations.

- Federal Entities: Incident Reporting and the Notification to federal regulatory entities including the Internal Revenue Service (IRS), Treasury Inspector General for Tax Administration (TIGTA), Social Security Administration (SSA), Federal Bureau of Investigations (FBI), Health and Human Services (HHS), etc., will be made by the impacted Agency Executive Director or the DTS CISO according to the specific requirements of each federal entity.
- State and local government: Notification will be made by the Agency Executive Director, or the DTS Chief Information Officer (CIO).
- Print and broadcast media: Notification will be made by the Agency Public Information Officer (PIO) or the DTS Public Information Officer (PIO).

All incident reporting and notification must be approved by the impacted Agency Executive Director, and/or the DTS Chief Information Officer, unless specifically allowed under state or federal regulatory statute.

- **FTI:** The unauthorized inspection or disclosure of Federal tax information (FTI), including breaches and security incidents, will be reported immediately by the DTS CISO or the appropriate Agency as listed below to the appropriate Agent-in- Charge, Treasury Inspector General for Tax Administration (TIGTA) and the IRS Office of Safeguards using the procedures outlined in section 1.8, IRS Publication 1075.
- Department of Human Services, Office of Recovery Services for FTI breaches in the ORS applications or databases.
- Utah State Tax Commission for FTI breaches in the TAX applications or databases.
- Department of WorkForce Services for FTI breaches in the DWS applications or databases.
- The agency will contact TIGTA and the IRS immediately, but no later than 24-hours after identification of a possible issue involving FTI. The agency should not wait to conduct an internal investigation to

determine if FTI was involved. If FTI may have been involved, the agency must contact TIGTA and the IRS immediately.

- **PCI:** The unauthorized inspection or disclosure of Payment Card Information (PCI), will be reported by the DTS CISO to the PCI Compliance Coordinator at the Utah State Department of Finance.
- **HIPAA:** The unauthorized inspection or disclosure of Personal Identification Information (PII) and/or Personal Health Information (PHI) related to a covered entity under HIPAA, including breaches and security incidents, will be reported by the DTS CISO or the appropriate Agency as listed below, without unreasonable delay and in no case later than 60 days from the discovery of the unauthorized disclosure to the Secretary of the U.S. Department of Health and Human Services using procedures outlined in the Breach Notification Rule.
- Department of Human Services, Office of Recovery Services for HIPAA breaches in the ORS applications or databases.
- Utah Department of Health for HIPAA breaches in the DOH applications or databases.
- **SSA**: If your agency experiences or suspects a breach or loss of PII or a security incident, which includes SSA-provided information, they must notify the State official responsible for Systems Security designated in the agreement. That State official or delegate 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 1-877-697-4889 (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 EIEP is to contact SSA's Office of Information Security, Security Operations Center, at 1-866-718-6425. The EIEP will provide updates as they become available to SSA contact, as appropriate. Refer to the worksheet provided in the agreement to facilitate gathering and organizing information about an incident.
- **FPLS/CS**: If Federal Parent Locator Service (FPLS) or Child Support (CS) information has been breached, in either electronic or physical form, the State CS agency must be notified immediately. The State CS agency-the Office of Recovery Services (ORS)-must alert the FPLS ISSO immediately upon discovery, but in no case later than one hour after discovery of the incident. The State CS agency reports the result of the investigation, mitigation, and resolution to the FPLS ISSO.
- **CJIS**: The unauthorized inspection or disclosure of Criminal Justice Information, will be reported by the DTS CISO or the appropriate Agency CJA ISO to the FBI CJIS Information Security Officer.

Incident Response Methodology

The Incident Response Methodology is a set of general guidelines that describes the principal phases of the incident response effort, and what happens during each phase. A set of step-by-step response procedures, specific to individual incident types will be created over time, and included in the On-line Security Notification form as they are developed.

The five principal phases of the CSIRP are as follows:

Alert Phase:

The alert phase is the process of learning about a (potential) security incident, and reporting it to the CISO and/or the DTS-Office of Enterprise Security.

Alerts may arrive from a variety of sources including: firewalls and intrusion detection systems, anti-virus software, threats received via electronic mail, media reports about a new threat, etc. The steps taken by the EISO may differ based on the information source.

Notification from Agency customers that their equipment may be experiencing abnormal behavior should be reported through ServiceNow tickets.

- Laptop/desktop tickets should be directed to Edge Support
- Server tickets should be directed to DevOps.

As the initial DTS investigations progress, if the potential of a security breach is found, Enterprise Security should be notified. Security's initial actions will handle the situation as an investigation. The Federal rules of evidence will be followed to maintain the chain of custody documentation. A forensic image of the subject system will be taken. As the severity of the situation unfolds, it may be upgraded to a security incident.

Notifications from the Security Operations Center (SOC) or from external sources such as the MS-ISAC SOC are handled directly by the Security Operations team. The types of events from firewalls, routers, switches, IDS, IPS, and web content filter include, but are not limited to:

- Reconnaissance
- Enumeration
- Denial of service
- Malware
- Intrusion
- Unauthorized access
- Web defacement
- Information spillage
- System malfunction
- Unencrypted traffic (regulated data in clear text)
- Unacceptable use

Triage Phase:

The triage phase is the process of examining the information available to determine if a legitimate incident occurred. The EISO will examine the information to make an initial assessment. If it is determined that federally regulated data exists on the system, the agency which owns the regulated data will be notified and approval to proceed granted. The Federal Rules of Evidence will be followed to maintain the chain of custody. A forensic image of the subject system will be taken.

When the EISO validates the probability of an incident, the CSIRT will be notified. The CISO with the assistance from designated CSIRT members will declare whether an incident has occurred and assess the scope and severity of the incident. If the incident severity is determined to be 4 or 5, the DTS CIO, COO, and PIO will also be alerted in this phase. The DTS CIO, COO, PIO, and CISO constitute the executive management board and must determine two important things in this phase:

- A decision to “pursue” or “protect” must be made. In other words, does the State of Utah want to attempt to catch the perpetrator(s) of the attack for later criminal or civil action, or does it simply want to

stop the incident and restore normal operations? This decision must be made before the response begins, because it influences how the response will happen.
- Resources (personnel and financial) must be allocated to the response and recovery teams at a level appropriate to the severity of the incident.
- Formal documentation and reporting during this phase will be managed by DTS-Enterprise Security.

Response Phase:

In the response phase, the CSIRT gathers evidence (audit trails, log files, contents of files, etc.). If the “pursue” option was chosen, this process must be performed in a forensically sound manner so that the evidence will later be admissible in court. Once evidence has been gathered, it will be analyzed by the CSIRT to determine the cause of the incident, the vulnerability or vulnerabilities being exploited, how to eliminate these vulnerabilities and/or stop the incident, and so forth. An assessment will also be made of how far the incident has spread (i.e., which systems are involved, and how badly have they been compromised).

- The CISO will assume the role of the CSIRT manager with authority to delegate responsibility across functional areas of the response team and establish expectations.
- Communications about the incident will be controlled and limited to members of the CSIRT and the Executive Management Board consisting of the CIO, COO, PIO, and CISO.
- Formal documentation and reporting during this phase will be managed by DTS-Enterprise Security.

Recovery Phase:

The recovery phase will begin once the response phase has been completed. In this phase, the CSIRT restores the systems affected by the incident to normal operation. This may require reloading data from backup files, or reinstalling systems from their original distribution media. Once the affected systems have been restored, they will be tested to make sure they are no longer vulnerable to the attack(s) that caused the incident. They will also be tested to make sure they will function correctly when placed back into production.

- The CISO will determine the completion of each phase and approve operational requirements.
- Formal documentation and reporting during this phase will be managed by DTS-Enterprise Security.

Maintenance Phase:

The maintenance phase is also called “lessons learned.” In this phase, the entire incident, as well as the response, will be reviewed to determine which parts of the CSIRP plan worked correctly, and which parts need improvement. The areas in which improvement is needed will be corrected, and the CSIRP updated accordingly. Other areas that need to be changed (policies, system configurations, etc.) may also be identified during this phase.

Formal documentation and reporting during this phase will be managed by DTS-Enterprise Security.

Appendix A

The Cyber Security Incident Response Team

The Cyber Security Incident Response Team (CSIRT) has the responsibility to respond to computer related security incidents. The CSIRP delegates authority to implement necessary actions and decisions before, during, and after an incident to the CISO and the CSIRT.

The following sections define the responsibilities and expectations of the CSIRT:

Mission:

The CSIRT is tasked with responding to all designated security incidents in a timely and professional manner. CSIRT members are expected to maintain high standards of personal and professional ethics. The primary mission of the CSIRT is to protect information assets belonging to state agencies and the public those agencies serve, while minimizing the impact of the CSIRT on operational requirements, and collecting data and evidence for prosecution.

Scope:

The CSIRT serves all state agencies, information asset stakeholders, and the general public. The CSIRT is responsible to protect all state networks and information assets, including networks connected to the state network.

Organizational Structure:

The CSIRT reports directly to the CISO. Members of the CSIRT include technical professionals from the DTS Enterprise Networking, DevOps, and Edge Support groups as well as software development professionals, database administrators, and security analysts. Each member of the CSIRT is appointed by the Executive Management Board and serves at the discretion of their normal supervisor/manager.

Services Provided:

Specific services the CSIRT provides are defined by the CISO as dictated by the requirements of the incident response.

Roles and Responsibilities

CISO

The CISO will assume the role of CSIRT Manager (or Leader) and is responsible for managing the overall response and recovery activities for all security incidents. The CISO will determine (with assistance from other CSIRT members) the severity of each incident, and decides which staff members will perform the actual response and recovery tasks.

Executive Management Advisory Board

The management advisory board includes the DTS-CIO, COO, PIO, CISO, and other delegates as directed by the Chief Information Officer.

Media Relations

All media relations associated with an incident response effort will be coordinated and approved by the DTS-PIO.

Permanent Team Members

Permanent team members include IT staff whose primary job responsibility is IT security. Security Analysts working in the Enterprise Security groups are included in the CSIRT. Permanent Team Members will be the initial responders to any designated security incident.

Temporary Team Members

Temporary team members report to DTS-Infrastructure and Application Development groups, and other internal business units or Agencies as directed by the management advisory board. They can include the Agency Public Information Officer and subject matter experts for the particular systems, applications, and business issues involved in the incident. Temporary team members are assigned to the CSIRT by their normal supervisors and/or managers at the request of the CISO, and serve for the duration of the incident.