Incident Response Plan

Document Name: Incident Response Plan

Department: Information Technology, Ethics & Compliance

Focus Area: Entire University

1. Statement

This incident response plan follows Utah State University's Information Security and Appropriate Use Policy 550, guiding students, faculty, and staff in protecting the confidentiality, integrity, and availability of Institutional Data across all formats and storage methods, both digital and physical.

2. Purpose and Goals

The Incident Response Plan (IRP) provides a clear framework for identifying, assessing, responding to, communicating about, and documenting **Information Security Incidents** efficiently.

The goals of an Incident Response Plan (IRP) is to minimize the impact of security incidents, identify their causes to prevent recurrence, preserve information for analysis and notification, clarify responsibilities, ensure proper reporting, comply with data breach laws, and safeguard the university's reputation.

3. Definitions

3.1. Information Security Incident: Information Security Incident refers to events—both electronic and non-electronic—that negatively impact institutional data at Utah State University. This includes unauthorized access, acquisition, disclosure, loss of access, or destruction of data, regardless of format or storage medium. However, this IRP specifically addresses information security incidents, not those caused by natural disasters, power failures, or other non-security-related disruptions.

These incidents can encompass different types of data (See USU Institutional Data Classification).
Examples:

- Attempts to gain unauthorized access to systems or data, whether successful or not.
- Theft or loss of devices containing sensitive information, regardless of ownership.
- Disruptions or denials of service.
- Unauthorized use of systems for data processing or storage.
- Changes to system hardware, firmware, or software without the owner's consent.

4. Scope

This IRP applies to all units and colleges within Utah State University. Specifically, the scope of this Incident Response Plan encompasses:

A. Faculty, staff, and all units

B. Third-party vendors who collect, process, share, or maintain university institutional data, whether managed or hosted internally or externally;

C. Personally owned devices of faculty, staff, and all units that access or maintain Institutional Data.

5. Policy

A. All faculty, staff, and workforce members are required to report any information security incidents to one of the following: IT Service Desk, USU's Hotline Reporting System, the Office of General Counsel, the Chief Information Security Officer (CISO), or the Data Privacy Officer.

B. Incidents must be reported as soon as possible but no later than **48 hours** from the time they are initially detected.

C. Some Information Security Incidents may also be criminal in nature (e.g., threats to personal safety or physical property) and should immediately be reported to the USU Department of Public Safety and concurrent with the incident report described above.

D. To avoid inadvertent violations of state or federal law, individuals and departments may not release information, electronic devices, or electronic media to any outside entity, including law enforcement organizations, before making the reports required by this incident response plan.

E. Information related to Information Security Incidents is considered High-Risk information.

F. When university staff report, track, and respond to Information Security Incidents, they must protect and keep confidential any **High-Risk information**.

G. Incident data retained for investigation will exclude any High-Risk information that is not required for incident response, analysis, or by law, regulation, or university policy.

6. Roles and Responsibilities

a) **The University Information Security Officer (ISO)** The final authority for understanding and carrying out this IRP (Incident Response Plan) lies with the Office of General Counsel, the Chief Information Security Officer (CISO), or the Data Privacy Officer They will maintain appropriate records and evidence related to significant incidents for a duration of three years from the time the incident took place. In cases where there is an unauthorized disclosure of PHI (Protected Health Information), records will be retained for an extended period of six years[1].

b) **The Information Assurance Team (IAT)** initially handles all reported incidents. The IAT is integrated by the University Institutional Security Officer (ISO), the Chief Privacy Officer, unit Compliance Owners, and a representative from the Office of General Counsel The IAT will oversee, coordinate, and guide the incident management process to promote a consistent, efficient, and effective response, including compliance with applicable breach notification laws and regulations. In addition, the IAT shall:

1. Convene, when appropriate, a multi-department Incident Response Team (as defined in USU Policy 5200)
2. Collaborate and coordinate with other university offices including applicable compliance

[1] General Records Schedule (GRS) 24 specifies that incident handling records should be kept for three years. See Page 56: https://www.archives.gov/files/records-mgmt/grs/grs-transmittal-24.pdf

offices.

3. Take appropriate steps to preserve forensic evidence.
4. Lessons learned meetings will be conducted for all serious Information Security Incidents to review the effectiveness of the incident handling process, prevent the recurrence of similar incidents, and identify potential improvements to existing security controls and practices.
5. Conduct ongoing Data Incident reporting education and awareness for the USU community.

c) **Data Users:** All faculty, staff, and workforce members must report Information Security Incidents to the IAT , IT Service Desk, or the USU's Hotline Reporting System within 48 hours of becoming aware of the incident. For additional information about Data Users visit USU Policy 5200.

d) **Compliance Owners:** Compliance owners are individuals with subject matter expertise and assigned responsibilities to lead compliance efforts within specific areas. At USU, they may serve as Data Trustees or Data Stewards, as outlined in USU Policy 5200.They will appropriately support the IAT and the IRT in incident handling and post-incident investigations and will evaluate and respond to Information Security Incidents in accordance with university and unit policies and procedures.

e) **Incident Response Team (IRT):** When appropriate, the IAT will convene this multi-department team whose primary objective is to assess and guide the University's response to IT security or privacy incidents to comply with existing data breach notification requirements and processes and determining whether individuals should be notified of a breach affecting their personally identifiable information. The IRT serves as a vital resource in managing incident response and mitigating potential harm to individuals and the institution. The IRT team members include:

1. Information Security Officer
2. The Information Assurance Team (IRT)
3. Compliance Owners
4. Unit System Administrators or Support Technicians.
5. Chief Compliance Officer
6. Data Stewards
7. A representative of the Office of Legal Affairs
8. A representative from the University Marketing and Communications (UMAC)
9. Vice President(s) from the affected units
10. USU Police Department
11. Others

As per the type and scale of the incident, the IRT team members may seek assistance from other university personnel who possess expertise and knowledge relevant to the incident's nature and scope. These guest members are crucial in offering support, guidance, and specialized insights from their respective areas of expertise. Such individuals may include, but are not limited to, department administrators or subject matter experts.

f) **Third-Party Vendors and Contractors:** USU has an ownership, stewardship, or custodial interest in all university data, regardless of how or where it is stored, transmitted, or processed. The reporting requirements of this Incident Response Plan apply to third parties that are contractually bound to limit the access, use, or disclosure of USU information assets. These third-party vendors or entities shall report potential or actual incidents to the university per the terms of their contract and/or the university's Data Processing Agreement (DPA), or equivalent.

7. Communication During an Incident

Units should rely on the IAT to manage and coordinate communication during an incident—both within the group of people working on the incident and on any notifications to leadership, users, or others. The IAT will ensure the appropriate communication cadence and level of detail, so people have the information they need and are not unduly alarmed, and that the investigation is not jeopardized. Units are asked not to communicate about an incident without first working with the IAT.

8. Incident Lifecycle

The incident lifecycle processes are depicted in **Figure 1 below**. They include the following:

8.1. Incident Detection and Reporting

The incident detection process involves observation of malicious or anomalous activity and gathering information that provides insight into security threats or risks. Reports of threats from sources external to USU may also trigger an incident report.

Information Security Incidents that are detected by any USU Data Users can be reported through the following channels:

- Directly to the IAT members
- Through IT Service Desk: T 435.797.HELP (4357), **servicedesk@usu.edu**, or
- USU's Hotline Reporting System

As noted above, incidents should be reported as soon as possible but no later than 48 hours from the time they are initially detected.

Third-party vendors and Contractors shall report potential or actual incidents to the university per the terms of their contract and/or the university's Data Processing Agreement (DPA), or equivalent.

The IAT shall:

a) Ensure that all staff are equipped with the necessary training, tools, and procedures to identify Information Security Incidents and breaches.

b) Provide ongoing guidance and expertise to unit staff to support incident response readiness.

c) Regularly perform comprehensive risk assessments to identify vulnerabilities and potential security threats.

d) Maintain updated contact lists for all relevant stakeholders, including legal, public relations, and external agencies like law enforcement.

8.2. Identify Incident Severity Classification

When a Data Incident is reported through the IT Service Desk or USU's Hotline Reporting Systems, or directly to the IAT , the administrator of these systems is responsible solely for reporting the incident to the IAT . Upon notification, the IAT will then evaluate the type of incident and proceed with the appropriate response based on the nature of the incident. For that purpose, the IAT will complete the **Incident Response Report and Risk Factor Analysis** (see Attachment 1), documenting all relevant details of the incident. Store all documentation centrally (e.g., Box) for easy access, future reference, and reporting.

This **Incident Response Report and Risk Factor Analysis** helps evaluate the significance or severity of the incident based on predefined criteria and defines clear thresholds for incident escalation within the organization.

8.3. Incident Response Process

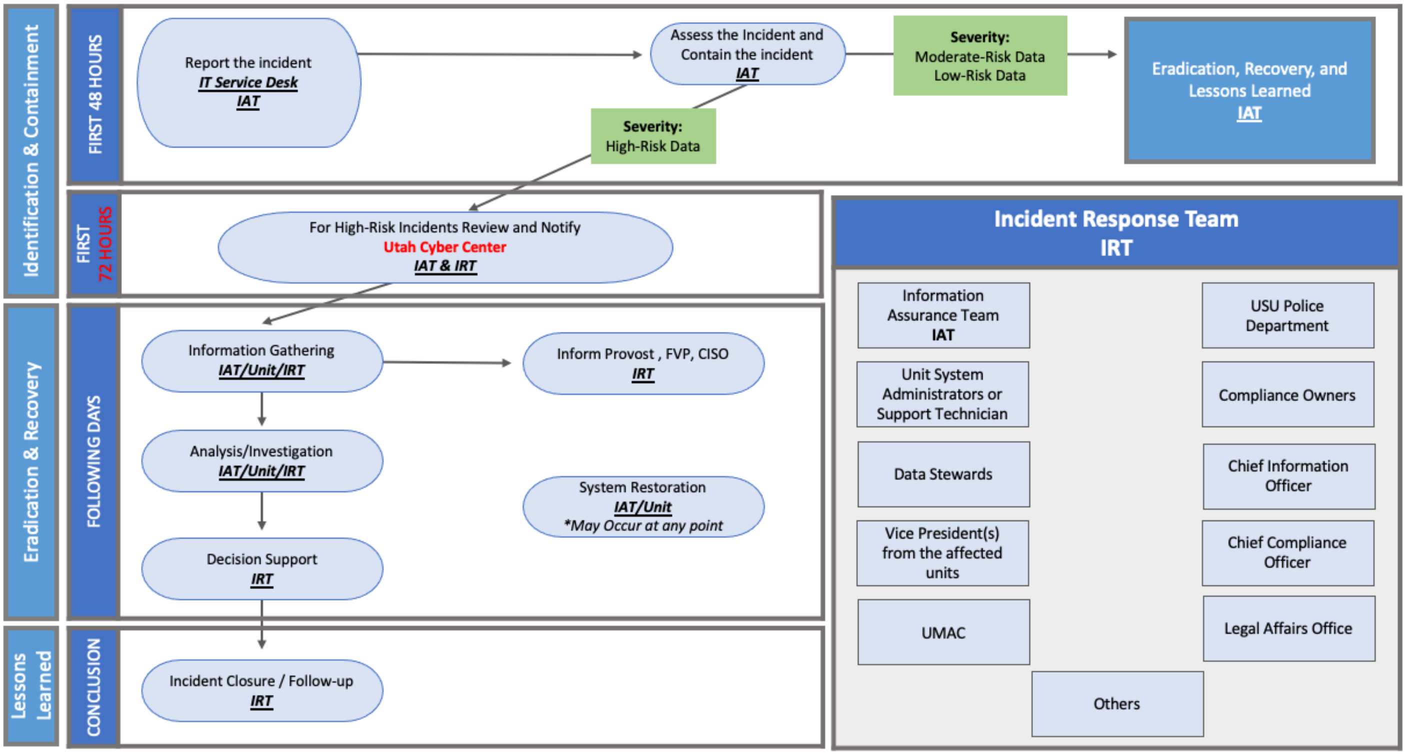
The Incident Response Process is designed to provide a high-level guide for effective planning, communication, and response in the event of a Data Incident.

Stage	Information Assurance Team (IRT) Actions and Procedures
Preparation	• **Training and Tools:** Ensure that all staff are equipped with the necessary training, tools, and procedures to identify, contain, and remediate Information Security Incidents and Data Breaches. • **Primary Responder Role:** Act as the primary responder for all Information Security Incidents, coordinating actions and delegating tasks as necessary. • **Risk Assessment:** Regularly, with the support of USU IT Services perform comprehensive risk assessments to identify vulnerabilities and potential security threats.
Identification	• Documentation: Complete the Incident Response and Risk Factor Analysis Report (See Attachment 2), documenting all relevant details of the incident. Store all documentation centrally (e.g., Box) for easy access, future reference, and reporting. • **Assessment of Severity:** Evaluate the significance or severity of the incident based on predefined criteria. • **Thresholds for Escalation**: Define and communicate clear thresholds for incident escalation within the organization. • **Communication:** Coordinate the identification process and, if necessary, inform appropriate compliance owners and leadership. • **Mandatory notification:** Elaborate and maintained an updated list of data breach notification laws applicable to USU data (See Attachment 3)
Containment	• **Guidance for Containment:** Provide specific guidance on effective strategies and actions for containing both Information Security Incidents and Data Breaches, ensuring minimal impact.
Eradication	• **Incident Analysis and Evidence Collection:** Analyze the incident, collect forensic evidence, and notify affected parties if device(s) or data need eradication.

	• **Guidance for Non-High-Risk Incidents:** Offer direction on eradication strategies for incidents that do not involve high-risk data. • **High-Risk Information Security Incidents:** Notify the Incident Response Team (IRT) if the incident involves high-risk data.
Recovery	• **System Restoration:** Ensure that affected systems are restored to normal operational status and are secure against similar incidents. • **Enhancement Suggestions:** Provide recommendations for system hardening and oversee the implementation of such measures. • **Information Sharing:** Communicate findings and recovery status with all involved parties. • **High-Risk Incident Oversight:** Specifically review and adjust recovery plans for incidents involving high-risk data, maintaining compliance with regulatory requirements.
Lessons Learned	• **Documentation and Review:** Document findings and lessons learned from the incident. For incidents involving high-risk data, organize a debriefing session involving relevant parties to discuss the incident management process. • **Regular Drills:** Conduct regular simulation exercises to test and refine the IRP, training staff on their roles during an incident. Establish mechanisms for gathering and incorporating feedback from all participants in an incident or drill.

FIGURE 1

Quick Reference Guide: Incident Response Plan



9. Additional Information

Specific guidelines, procedures, standards, and best practices for secure computing can be found at:

- 5200: Information Security
- 5201: Appropriate Use of Computing, Networking, and Information Resources
- 5202: Uniform Wired and Wireless Data Networks
- 5203: Internal Bulk Email
- 5204: Banner Identification Number
- 5205: Network Monitoring & Vulnerability Scanning Policy
- 5207: Institutional Email Service

Additional information can be found at:

USU Institutional Data Classification
Data Breach Notification Obligations Table for Higher Education Institutions PDF