Utah Tech University Policy

463 B: Incident Response Procedure

I. Summary

1.1 As defined in Utah Tech University ("the University") Policy 463, this Incident Response Procedure ("Procedure") defines roles and action in the event that a security incident reaches a level that warrants formal response. This Procedure is based in part on guidance from the National Institute of Standards and Technology (NIST) Special Publication 800-61 (SP800-61), Computer Security Incident Handling Guide.

1.2 Incident Response will focus on four areas of the lifecycle of a security incident:

1.2.1 Preparation

1.2.2 Detection and Analysis

1.2.3 Containment, Eradication, and Recovery

1.2.4 Post-Incident Activity

1.3 This Procedure also outlines the actions to be taken when incidents involving the breach or inappropriate disclosure of confidential personal information, or which otherwise create circumstances where public notification or acknowledgement of the incident is required.

II. Procedure

2.1 Incident Response Team – the University does not maintain a full-time incident response team. As defined in Policy 463, in the event a formal response to an information security incident(s) is required, an ad-hoc incident response team (IRT) will be convened to perform these activities. The Information Security Officer or another designated member of the Information Security Office (ISO) will act as the team incident commander and will direct incident response activities.

2.1.1 This team will consist of any necessary members to effectively respond to the incident(s), including technical staff, personnel from affected departments, and other specialized subject-matter experts. Depending on the size and scope of the incident, team members

may include, but are not limited to, representation from the following University roles: Information Security Officer (ISO), Data Trustee(s), Data Steward(s), system or network administrators, public relations, legal counsel, risk management, and University police.

2.1.2 Outside entities may also be deemed necessary to incident response and may be involved in the incident response team, including but not limited to, affected vendors or contractors, cyber-insurance providers, outside legal counsel, security and forensic consultants, and external law enforcement agencies.

2.2 The incident response team is responsible for all incident response actions during an active incident response event, including communication with the University community and outside entities. The team will coordinate with University Administration and/or affected departments to ensure that sufficient resources are available to successfully perform incident response activities.

III. Preparation

3.1 As it is impossible to prevent or foresee all potential security incidents, ISO is responsible for maintaining a state of readiness to respond to security incidents. ISO will coordinate with expected ad-hoc incident response team members before incidents occur to ensure smooth and timely transitions when incident response is needed.

IV. Detection and Analysis

4.1 There is no limit to the ways a security incident requiring formal response can occur. Detection of an incident may occur through technical or non-technical means. An incident may occur as a single event or as a culmination of several smaller, less serious events. Incidents may be discovered internally or reported by external entities.

4.1.1 ISO will analyze detected and/or reported security incidents. In the event an incident requires formal response, ISO will convene necessary members of the University incident response team. Documentation of the incident and any response activities will be maintained.

4.1.2 ISO and/or the incident response team will prioritize incidents and communicate to University administration and/or affected departments that incident response procedures have begun.

V. Containment, Eradication, and Recovery

5.1 Containment efforts are intended to identify, limit, and prevent further damage from active threats to University information and infrastructure posed by a security incident. Once an incident has been detected or reported, Security Incident Responders will work through technical means to identify and contain any elements or agents that may actively be operating within or against the University information technology environment; e.g., active malware or a distributed denial of service (DDoS) attack. Such means of containment may include, but are not limited to, disabling user accounts, isolating client devices, servers, or network infrastructure, limiting or disabling internal network or Internet access, and so on. Typically, containment measures will be temporary until the threat has passed, but in some cases may become permanent if necessary to prevent further incidents.

5.2 The incident response team will inform and consult with University administration on containment measures, which may have an impact on operations or University functions. The incident response team and ISO reserve the right to unilaterally implement containment measures during an active incident, as needed, to contain active threat elements, prevent loss of information assets, and limit further damage to University systems and infrastructure. In such cases, these measures will be communicated after the fact to administration and re-evaluated after the threats are contained.

5.3 Eradication and recovery efforts are intended to remove any residual elements of a security incident and restore University operations and infrastructure to its normal, pre-incident state. The incident response team will oversee any needed eradication and recovery efforts.

VI. Post-incident Activity

6.1 Post-incident, ISO, members of the incident response team, affected departments, University administration, and other relevant parties will review the incident. Typically, this will be a 'lessons learned' meeting covering, but not limited to, the following topics:

6.1.1 Review the details of the incident

6.1.2 Identify root causes of an incident

6.1.3 Identify gaps in policies, procedures, or technical controls that may have allowed the incident to occur

6.1.4 Identify corrective actions to prevent similar incidents

6.1.5 Review performance of the incident response team

VII. Reporting of Information Security Incidents

7.1 In some circumstances as defined by University Policy 463, Federal and State law, contractual obligations of the University, or public relations practices may require that the incident be reported publicly. Any incident in which it is discovered or reported that Restricted information has been breached or inappropriately disclosed will typically by law require a breach notification to affected persons and entities. Additionally, some incidents not involving Restricted data may still warrant a public notification or acknowledgement of the incident; for example, Web defacements, or sustained DDoS attacks that impact or degrade University technical operations or public-facing services.

7.2 Verification that an incident meets the legal or contractual requirements to notify, and notification efforts should begin as early as reasonably possible during the incident lifecycle, in tandem with containment, eradication, and recovery efforts. Notification requirements and timing may also be driven by Federal and/or State law regulations. The incident response team, including general counsel, public relations, and ISO, will work closely with University administration and affected departments to determine:

7.2.1 What Restricted information may have been breached or disclosed; e.g., social security numbers, credit card numbers, non-directory FERPA information, etc.

7.2.2 What the impact of the breach is on affected persons or entities.

7.2.3 Develop a notification strategy and timeline for informing affected people and entities of the breach and the University's response.

7.2.4 Develop public relations material and prepare to handle increased media coverage and communication from affected persons.

7.2.5 Determine what services or offerings to affected persons or entities may be required as a result of the breach.

7.3 Notification letters or other communication sent to affected persons and entities must be signed by the responsible Data Trustee or other highest-level administrator for the department or unit responsible for the Restricted Data that was breached, as appropriate, unless otherwise

determined by University Administration.

Policy Owner: Vice President of Administrative Affairs
Policy Steward: Chief Information Officer

History:
Approved 11/10/23
Revised 0/0/00