Procedure P4-004N: IT Security Incident Management

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this IT Security Incident Management Procedure is to outline the requirements of an IT Security Incident management plan as a means of minimizing the impact of IT Security Incidents, protecting University Assets, and ensuring a swift and coordinated response.

B. Scope.

The scope of this procedure is all University administrative units, including colleges, divisions, departments, and centers, and all members of the University community, including students, staff, faculty, other permanent or temporary employees, contractors, research collaborators, vendors, and third-party agents.

This procedure supports Section N, titled IT Security Incident Management, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this procedure. In addition, the terms below apply for the limited purpose of this procedure.

A. Incident Response Team (IRT) – An authorized group of IT professionals responsible for preparing for and responding to IT emergencies.
B. Information Security Office (ISO) – The University's information security department, which reports to the chief information security officer (CISO).

III. Procedure

A. All members of the University community shall immediately report any suspected or detected IT Security Incidents to their respective help desk.

B. The chief information security officer (CISO) or their designees shall direct IT Security Incident response efforts.

C. The Incident Response Team (IRT) shall coordinate with University administrative units and entities at the direction of the Information Security Office (ISO) regarding IT Security Incident handling and communication.

D. IT managers, IT Technicians, and Users managing Assets shall take the following actions in reaction to suspected or detected IT Security Incidents:

1. Immediately disconnect the Information Systems from the network; do not run any applications, antivirus/anti-malware scans, or other tools; and do not power off the Information Systems.

2. Contact the ISO and discontinue use until further instruction from the ISO.

3. Outside of business hours, IT managers and IT Technicians shall submit a high-priority ticket to the ITS Service Desk (801-587-6000) to start the Security Operations Center (SOC) escalation process.

E. The ISO shall create and maintain an IT Security Incident response plan.

1. The IT Security Incident response plan shall include, at a minimum, the following:
    a. roles and contact information;
    b. identified primary and alternative communication channels;
    c. detection, reporting, and analysis processes;
    d. evidence collection and retention processes;
    e. containment and eradication processes;
    f. recovery processes; and
    g. post-IT Security Incident communication and review processes, including documentation and lessons learned.

F. The ISO shall test and update the IT Security Incident response plan on at least an annual basis.

Sections IV- VII are for user information about this procedure.

IV. Policies/ Rules, Procedures, Guidelines, Forms and other Related Resources

A. Policies/ Rules.

1. Policy 4-004: University Information Security Policy

B. Procedures, Guidelines, and Forms. [*reserved*]

C. Other Related Resources.

V. References

[*reserved*]

VI. Contacts

The designated contact officials for this Regulation are:

A. Policy Owner(s) (primary contact person for questions and advice): Chief Information Security Officer

B. Policy Officer(s): Chief Information Officer

See Rule 1-001 for information about the roles and authority of policy owners and policy officers.

VII. History

Revision History.

A. Current version. Revision 0.

1. Approved by Chief Information Security Officer with effective date of November 6, 2024.

B. Renumbering

1. Not applicable