Procedure P4-004I: Network Security

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of this Network Security Procedure is to outline the steps required to ensure the confidentiality, integrity, and availability of the University's network.

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 I, titled Network Security, 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. External Network – A network not controlled or administered by the University.

B. GRC – The Information Security Office's (ISO) Governance, Risk & Compliance team. Contact: ISO-GRC@utah.edu.

C. IAM – The Information Security Office's (ISO) Identity & Access Management team. Contact: IAM-team@utah.edu.

D. Information Security Office (ISO) – The University's information security department, which reports to the chief information security officer (CISO).

E. Internal Network – A network controlled or administered by an employee of the University.

F. Least Privilege – The principle of granting Users the minimum access and authorization needed to perform their job functions.

G. Network Access Control (NAC) – A generic term for an IT solution to selectively grant network access to devices and Users based on one or more criteria (e.g., authentication and security configuration).

H. Segment (or Segmentation) – The physical and/or logical separation of networks at multiple layers to provide confidentiality, integrity, and availability to a network.

III. Procedure

A. All University network traffic shall enter and exit the University network through a managed border firewall and have an inbound default-deny rule in place. Other points of entry and exit, or the removal of an inbound default-deny rule, shall be approved by the chief information security officer (CISO) and the chief technology officer (CTO). For additional information, contact GRC.

B. All vendors providing support to University Information Systems shall use the ISO-approved Remote Access solutions wherever technically feasible. For additional information, contact IAM.

C. University networks shall be maintained using the principles of separation of duties and Least Privilege.

D. IT managers shall:

1. maintain a current and accurate inventory of all Assets for which they are responsible;
2. register their point of contact (POC) information for all network assignments for which they are responsible in the POC application in the University's IT Service Management (ITSM) platform;
3. establish a comprehensive Patch management plan that aligns with Policy 4-004 and Rule R4-004G;
4. For more specific implementation requirements, please access Rule R4-004G.
5. coordinate with the ISO on all suspected or detected IT Security Incidents for reporting, containment, eradication, and recovery measures;
6. be knowledgeable of and accountable for the regulatory requirements and industry standards related to networks for which they are responsible, such as PCI DSS, HIPAA, FERPA, etc.;
7. conduct at least annual assessments to identify areas for improvement and ensure compliance with all applicable federal, state, and local laws, regulations, and statutes, as well as contractual obligations; and
8. maintain comprehensive documentation and diagrams of network architecture (e.g., data flow and logical and physical design), configurations, internal procedures, and IT Security Incident response activities, and at least annually review and update them to reflect changes in the environment.

E. IT Technicians shall:

1. Segment the Internal Networks for which they are responsible using one or more of the following methodologies:

a. functional areas;

b. business unit, divisions, departments, schools, or colleges;

c. data types, business criticality, regulatory or contractual requirement; or

d. security zones to minimize the impact of IT Security Incidents and Unauthorized Access;

2. implement Network Access Controls (NAC), firewall rules, and intrusion detection/prevention systems for the networks for which they are responsible to restrict Unauthorized Access to Assets such that diverse network Segment traffic must traverse a firewall to communicate with another diverse Segment;
3. implement the ISO's authentication services for all Information Systems wherever technically feasible;
4. conduct regular Vulnerability assessments per Procedure P4-004G2 to identify, mitigate, and remediate Vulnerabilities in Information Systems for which they are responsible;
    a. For more specific implementation requirements, please access Procedure P4-004G2.
5. follow the Patch management plan established by the IT manager; and
6. where not in place by UIT, implement continuous network monitoring tools and logging for the networks for which they are responsible to promptly detect and respond to suspicious activities and anomalous behavior.
    a. For more specific logging implementation requirements, please access Rule R4-004J and Procedure P4-004J.
    b. For more specific IT Security Incident response implementation requirements, please access Procedure P4-004N.

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.

1. Point of Contact Service Request

V. References

A. Rule R4-004G: IT Resource and Information System Security and Vulnerability Management

B. Rule R4-004J: Log Management and Monitoring

C. Procedure P4-004J: Log Management and Monitoring

D. Procedure P4-004N: IT Security Incident Management

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