Procedure P4-004G1: Configuration Hardening

Revision 0. Effective date: November 6, 2024

I. Purpose and Scope

A. Purpose.

The purpose of the Configuration Hardening Procedure is to outline the process for managing and hardening Configurations of Information Systems according to Rule 4-004G.

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 G, titled IT Resource and Information System Security and Vulnerability Management, of the University of Utah Information

Security Policy 4-004 and Rule R4-004G, titled IT Resource and Information System Security and Vulnerability Management.

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. Configuration – The arrangement, management, and related documentation of components, hardware, software, and firmware. Along with its architecture, the Configuration of an Information System affects both its function and performance.

B. Configuration Hardening – The process of reducing the Vulnerabilities posed by an Information System's Configuration. This is an ongoing process that requires continuous monitoring for areas of improvement.

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

D. Security Benchmark – Prescriptive Configuration recommendations that represent the consensus-based effort of cybersecurity experts to help protect Information Systems against cybersecurity Threats. Security Benchmarks can be used to create a Security Baseline.

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

III. Procedure

A. The scope of Configuration Hardening should include, but not be limited to, the following:

1. networking hardware;
2. servers, storage arrays, and associated hardware;
3. operational technology (OT);

4. operating systems;
5. databases;
6. Applications (e.g., web servers and middleware commonly have Security Benchmarks available);
7. Workstations; and
8. Mobile Devices.

B. IT managers shall:

1. maintain a current and accurate inventory of all Information Systems for which they are responsible; and
2. identify Security Benchmarks to be adopted (e.g., the University primarily uses the CIS Security Benchmarks).

C. IT Technicians shall:

1. document the current Configuration state of each Information System for which they are responsible, including applied Security Benchmarks;
2. wherever technically feasible, leverage Configuration management tools to automate Configuration Changes, ensure consistency, and verify the extent to which the current Configuration of Information Systems aligns with the selected Security Benchmarks;
3. harden Information Systems by prioritizing critical Controls:
    a. control access;
        i. Role-based access and Least Privilege: Define account roles and assign each role the minimum amount of privileges necessary to perform job functions.
        ii. Identify and disable unnecessary accounts: Delete or disable inactive and unused accounts.

iii. Use the Information Security Office's authentication services. Where not technically feasible, enforce strong passwords and multifactor authentication (MFA): Configure Information Systems to require passwords that are, at a minimum, in compliance with Rule R4-004D and enforce MFA for all accounts.

For more specific implementation requirements, please access Rule R4-004D.

iv. Restrict and secure access: Limit access to nonpublic services only to computers connected to the University network. Secure Remote Access with strong Encryption.

b. minimize attack surface; and

i. Apply software updates: Identify and apply software updates on a regular schedule. Where practical, implement automated Patching.

ii. Implement network Segmentation: Architect Information Systems to isolate critical Assets from less sensitive ones through network Segmentation techniques.

For more specific implementation requirements, please access Procedure P4-004I.

iii. Identify and disable unnecessary services: Disable or remove ports, services, and Applications that are not needed. Configure host-based firewalls to block all incoming traffic on ports and services deemed unnecessary.

c. implement monitoring:

i. enable and retain logging;

ii. alert on suspicious activity; and

iii. alert on Configuration Changes.

For more specific implementation requirements, please access Rule R4-004J and Procedure P4-004J.

4. apply the applicable Security Benchmarks:
    a. compare the current Configuration to the Security Benchmark recommendations;
    b. understand the security recommendations and possible adverse effects contained within a Security Benchmark and the underlying rationale before release to a production environment;
    c. implement the applicable Security Benchmarks for each Information System for which they are responsible;
    d. document deviations from a Security Benchmark to allow for necessary functionality;
    e. validate that Security Benchmarks Changes have been applied and are functioning as expected; and
    f. regularly review new versions of the Security Benchmark and update Configurations accordingly; and
5. manage Vulnerabilities.

    For more specific implementation requirements, please access Procedure P4-004G.

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

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

C. Other Related Resources.

V. References

A. Rule R4-004D: Access Management

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

C. Procedure P4-004G: Vulnerability Management

D. Procedure P4-004I: Network Security

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

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