Rule R4-004F: Physical and Facility Security

Revision 1. Effective date: September 12, 2023

I. Purpose and Scope

A. Purpose

The purpose of this Physical and Facility Rule is to protect the University's premises and facilities by establishing requirements for secure operations.

B. Scope

The scope of this rule 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 rule supports section F, titled Physical and Facility Security Rule, of the University of Utah Information Security Policy 4-004.

II. Definitions

The definitions provided in Policy 4-004 apply for this rule.

III. Rule

A. Physical Security Perimeter

1. The following will be implemented as applicable for physical security perimeters:

    a. security zones will be clearly defined, and the Controls applied to each zone should be commensurate with the physical security requirements of the Information Systems contained within; and

    b. the security perimeters of a building must be physically sound and include the following protections:

        i. the external walls must be of solid construction;

        ii. the external doors must be protected against unauthorized access with appropriate Control mechanisms including locks and/or alarms;

        iii. doors and windows must be locked when unattended;

        iv. access to physical security zones and buildings will be restricted to authorized personnel only;

v. staffed reception areas are encouraged where appropriate to further control physical access to the building; and

vi. fire doors on a physical security perimeter must be alarmed and monitored.

B. Physical Entry Controls

1. To ensure that only authorized personnel have access to secure areas, the following physical entry Controls shall be implemented:

   a. a visitor log that records the following:

      i. visitor name;

      ii. visitor's date and time of entry;

      iii. visitor's organization;

      iv. the University personnel accountable for the visitor;

      v. the purpose of visit; and

      vi. the time of the visitor's departure.

2. Staff, faculty, other permanent or temporary employees, contractors, vendors, and visitors shall wear a form of visible identification.

3. Access to security zones where Restricted Data is stored or processed requires the following additional Controls to authenticate and validate authorized personnel:

   a. access Controls, such as access cards, control code panels, etc.;

   b. regular logging and monitoring of authorized access; and

   c. regularly reviewing, updating, and revoking authorized access as appropriate.

4. Unauthorized photographic, video, audio, or other recording equipment is prohibited in security zones.

C. Protecting Against Natural and Environmental Threats

1. All departments and units shall avoid damage from natural and environmental Threats by storing hazardous or combustible materials a safe distance from secure areas, providing and placing suitable fire-fighting equipment appropriate to the area, and maintaining back-up utilities, equipment, and media a safe distance from secure areas.

D. Information System Location and Protection

1. To further protect the University's IT Resources and Information Systems from natural and environmental Threats, IT Technicians shall implement the following Controls:

    a. Place IT Resources and Information Systems in a location with limited access;

    b. position IT Resources and Information Systems that store or process Restricted or Sensitive Data in a way that minimizes the ability of unauthorized people to view the equipment;

    c. isolate IT Resources and Information Systems that require special and/or elevated protection;

    d. adopt Controls to monitor and minimize the Risk of the following physical Threats as appropriate:

        i. theft;

        ii. fire and smoke;

        iii. water and humidity;

        iv. temperature fluctuations;

        v. vibration; and

        vi. electrical supply or other electrical interference;

e. ensure that the following supporting utilities are adequate for the Information Systems they are supporting:

   i. electricity;

   ii. water supply;

   iii. HVAC; and

   iv. back-up Uninterruptible Power Supply (UPS); and

f. ensure that only University Information Systems are plugged in to power outlets and/or network and communications ports in University data centers.

E. Cabling Security

1. To protect power and network cabling from interception or damage, IT Technicians shall implement the following Controls:

   a. where possible, power and telecommunication lines connected to University's facilities shall be underground;

   b. protect network cabling by utilizing conduit or avoiding routing network cabling through public areas;

   c. segregate power cables from network cabling to prevent interference;

   d. label cables to reduce handling errors; and

   e. network ports not in use shall be disabled.

F. Information System Maintenance

1. To ensure maintenance activities of the University's Information Systems that support availability and integrity are conducted in a secure manner, IT Technicians shall implement the following Controls:

   a. maintain equipment in accordance with the manufacturer's specifications;

b. confirm that maintenance personnel are authorized to conduct repairs and servicing of identified equipment;

c. require authorized maintenance personnel to fill out an entry and exit log for the facility when on-site repairs are conducted; and

d. keep records and/or logs of equipment faults and the resulting preventative and corrective maintenance.

Sections IV- VII are for user information and are not subject to the approval of the Academic Senate or the Board of Trustees. The Institutional Policy Committee, the Policy Owner, or the Policy Officer may update these sections at any time.

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

A. Policies/ Rules.

1. Policy 4-004: University of Utah Information Security Policy

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

C. Other Related Resources. [*reserved*]

V. References

A. 45 C.F.R. 164: Health Insurance Portability and Accountability Act (HIPAA): Security and Privacy

B. Family Educational Rights and Privacy Act of 1974 ("FERPA", 20 U.S.C. § 1232g)

C. Federal Information Security Management Act of 2002 ("FISMA", 44 U.S.C. § 3541)

D. ISO 27002:2013, Information Technology - Security Techniques - Code of Practice for Information Security Controls

E. NIST 800 Series, Federal Information Security Standards

F. Policy 3-070: Payment Card Acceptance

G. Policy 4-001: University Institutional Data Management

H. Policy 4-003: World Wide Web Resources Policy

I. Policy 5-111: Disciplinary Actions and Dismissal of Staff Employees

J. Policy 6-400: Student Rights and Responsibilities

K. Policy 6-316: Code of Faculty Rights and Responsibilities

L. Pub. 111-5, Division A, Title XIII, Subtitle D: Health Information Technology for Economic and Clinical Health Act (HITECH Act)

M. Omnibus HIPAA Rule: 45 CFR Parts 160 and 164 - Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the HITECH Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules; Final Rule

N. Utah Board of Higher Education Policy R345 Information Technology Resources Security

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 1.

1. Approved by President Randall as an Interim Rule on September 12, 2023 with effective date of September 12, 2023. Rule finalized with no changes after Board of Trustees approval of Policy 4-004 revisions on November 14, 2023.
2. Legislative History
3. Editorial Revisions

B. Previous Revisions

1. Revision 0. Effective date April 6, 2016.

C. Renumbering

1. Not applicable.