University Rule 4-004F: Physical and Facility Security Rev. 0.

I. Purpose and Scope

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

B. 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: University of Utah Information Security Policy, apply for purposes of this Rule, including the following:

A. **Confidential** - Any Information Asset which is classified as Restricted or Sensitive per the Data Classification and Encryption Rule.

B. **Information System** - An Application or group of servers used for the electronic storage, processing, or transmitting of any University data or Information Asset.

C. **Restricted Data** - Any data types classified as Restricted per the Data Classification and Encryption Rule.

III. Rule

A. Physical Security Perimeter

The following will be implemented as appropriate for physical security perimeters:

1. Security perimeter zones will be clearly defined and the controls applied to each zone should be commensurate with the security requirements of the Information Systems contained within.

2. The security perimeters of a building must be physically sound, to include the following protections:

    a. The external walls must be of solid construction.

    b. The external doors must be protected against unauthorized access with appropriate control mechanisms including locks and/or alarms.

    c. Doors and windows must be locked when unattended.

    d. Access to security zones and buildings will be restricted to authorized personnel only.

    e. Staffed reception areas are encouraged where appropriate to further control physical access to the building.

    f. Fire doors on a security perimeter must be alarmed and monitored.

B. Physical Entry Controls

To ensure that only authorized personnel have access to a secure area, the following physical entry controls will be implemented:

1. A log must be available to record the following Visitor activities:

    a. Visitor name

    b. Date and time of entry

    c. Visitor's organization

    d. The University personnel accountable for Visitor

    e. Purpose of visit

    f. Time of departure

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

3. Access to security zones storing or processing Restricted data will have additional controls to authenticate and validate authorized personnel:

   a. Access control examples include access cards, control code panels, etc.

   b. Authorized access will be logged and monitored.

   c. Authorized access will be regularly reviewed, updated, and revoked as appropriate.

   d. Unauthorized photographic, video, audio or other recording equipment are not allowed.

C. Protecting Against Natural and Facility Threats

To avoid damage from natural and facility threats, the following controls must be implemented:

1. Storage of hazardous or combustible materials must be maintained at a safe distance from secure areas.

2. Fire-fighting equipment appropriate to the area must be provided and suitably placed.

3. Back-up utilities, equipment and media must be maintained at a safe distance from secure areas to avoid damage from a disaster.

D. Information System Location and Protection

To further protect the University's Information Systems from natural and facility threats, the following controls should be implemented:

1. Assign equipment location to minimize unnecessary access into work areas.

2. Position equipment storing or processing Confidential data to minimize the line-of-sight viewing angle of unauthorized personnel.

3. Isolate equipment that requires special and/or elevated protection.

4. Adopt controls to monitor and minimize the risk of the following physical threats as appropriate:

   a. Theft

   b. Fire and smoke

   c. Water and humidity

   d. Temperature fluctuations

   e. Vibration

   f. Electrical supply or other electrical interference

5. Ensure that the following supporting utilities are adequate for the Information Systems they are supporting:

   a. Electricity

   b. Water supply

   c. HVAC

   d. Back-up UPS

6. 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

To protect power and network cabling from interception or damage, the following controls should be implemented:

1. Where possible, power and telecommunication lines into the University's facilities will be underground.

2. Protect network cabling by utilizing conduit or avoiding routing network cabling through public areas.

3. Segregate power cables from network cabling to prevent interference.

4. Cable labeling is encouraged to reduce handling errors.

5. Open ports shall not be utilized without authorization.

F. Information System Maintenance

To ensure maintenance activities of the University's Information Systems that support availability and integrity are conducted in a secure manner, the following controls should be implemented:

1. Maintain equipment in accordance with the manufacturer's specifications.

2. Confirm that maintenance personnel are authorized to conduct repairs and servicing of identified equipment.

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

4. Keep records and/or logs of equipment faults and the resulting preventative and corrective maintenance.

[Note: Parts IV-VII of this Rule (and all other University Regulations) are Regulations Resource Information--the contents of which are not approved by the Academic Senate or Board of Trustees, and are to be updated from time to time as determined appropriate by the cognizant Policy Officer and the Institutional Policy Committee, as per Policy 1-001 and Rule 1-001.]

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

A. Rules

TBD

B. Procedures

Policy 4-004 Procedures

C. Guidelines

TBD

D. Forms

E. Other Related Resource Materials

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: Code of 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

VI. Contacts

A. The designated contact Officials for this Policy are:

1. Policy Owner (primary contact person for questions and advice): Chief Information Security Officer, 801-213-3397

2. Policy Officer; Chief Information Officer, 801-581-3100

These officials are designated by the University President or delegee, with assistance of the Institutional Policy Committee, to have the following roles and authority, as provided in University Rule 1-001:

A 'Policy Officer' will be assigned by the President for each University Policy, and will typically be someone at the executive level of the University (i.e., the President and his/her Cabinet Officers). The assigned Policy Officer is authorized to allow exceptions to the Policy in appropriate cases.... "

"The Policy Officer will identify an 'Owner' for each Policy. The Policy Owner is an expert on the Policy topic who may respond to questions about, and provide interpretation of the Policy; and will typically be someone reporting to an executive level position (as defined above), but may be any other person to

whom the President or a Vice President has delegated such authority for a specified area of University operations. The Owner has primary responsibility for maintaining the relevant portions of the Regulations Library... .[and] bears the responsibility for determining -requirements of particular Policies... ." University Rule 1-001-III-B & E

VII. History

A. Current version: Revision 1, effective date: April 4, 2016

Approved by Academic Senate: May 4, 2015

Approved by Board of Trustees: May 12, 2015

Background information for this version