3364-65-03 Technology physical safeguards.

(A) Policy statement

The security of technology assets requires reasonable and appropriate physical security and environmental controls. The university secures its technology assets through measures designed to limit access to sensitive data to authorized users. These measures may include physical access controls, identity controls, computing environment controls, and logging controls.

(B) Purpose

This policy establishes policies to secure sensitive information processed, stored in computer rooms, network data closets, and telecommunication closets from equipment/data theft, vandalism, loss, and unauthorized access.

(C) Scope of policy

This policy applies to all university operating units and to any university partnerships, vendor/vendee relationships or other contractual relationships where sensitive information may be exchanged, accessed, processed, and otherwise disclosed.

(D) Definitions

(1) Device. As used in this policy, “device” shall retain its meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management Policy).

(2) Information technology asset. Information technology assets “IT assets” shall retain their meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(3) Sensitive data. Data for which the university has an obligation to maintain confidentiality, integrity, or availability.

(4) Technology asset. Technology assets shall retain their meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(5) Workstation. As used in this policy, "workstation" shall retain its meaning as defined in section (D) of rule 3364-65-05 of the Administrative Code (technology asset management).

(E) Policy

(1) Identity, access, and audit controls. Unaccompanied access to information technology facilities including all computer rooms, network data closets, and telecommunication closets is restricted to authorized personnel. Additional requirements for access and identity controls are established under rule 3364-65-02 of the Administrative Code (information security and technology administrative safeguards).

(a) Identity controls. Reasonable individual identification may be required before being granted access to university computing facilities.

(b) Visitor controls. Visitor access to locations housing technology assets may be restricted without notice.

(2) Contingency plans. The university will maintain procedures sufficient to allow physical access to its information systems in the event of an emergency or contingency scenario. Except as otherwise defined in policy or procedure, the university of Toledo's office of public safety procedures controlling the physical access to university facilities will govern such situations.

(3) Facilities and maintenance controls

The university will establish procedures safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft. The university documents repairs and modifications to the physical components of a facility which are related to security.

(4) Computing environment and workstation controls. The physical security requirements for devices and for workstations are established under rule 3364-65-06 of the Administrative Code (device and workstation).

(5) Asset lifecycle and disposal. The university has established policies and procedures to address the re-use and final disposition of technology assets. The disposal requirements for technology assets are established under rule 3364-65-05 of the Administrative Code (technology asset management).

(6) Recordkeeping. The university has established a requirement for the disposition of university technology assets to be reasonably known at all times. The recordkeeping requirements for technology assets are established under rule 3364-65-05 of the Administrative Code (technology asset management).

(7) Tampering with computing equipment. The university requires that assets which access, create, store, transmit, receive, or destroy sensitive data be reasonably guarded against tampering. Contact the information security office immediately if you suspect a technology asset has been tampered with.

Effective: 3/11/2019

CERTIFIED ELECTRONICALLY

Certification

03/01/2019

Date

Promulgated Under: 111.15
Statutory Authority: 3364
Rule Amplifies: 3364