Name of Policy: Technology Physical Safeguards **Policy Number**: 3364-65-03 **Approving Officer**: President **Responsible Agent**: Vice President, CIO/CTO **Scope**: All University organizational units			**Revision date:** November 19, 2018 **Original effective date**: October 11, 2007
☐	New policy proposal	☐	Minor/technical revision of existing policy
☒	Major revision of existing policy	☐	Reaffirmation of existing policy

(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 the Technology Asset Management Policy, University Policy Number 3364-65-05.

(2) Information Technology Asset. Information Technology Assets ("IT assets") shall retain their meaning as defined in section (D) of the Technology Asset Management Policy, University Policy Number 3364-65-05.

(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 the Technology Asset Management Policy, University Policy Number 3364-65-05.

(5) Workstation. As used in this policy, "Workstation" shall retain its meaning as defined in section (D) of the Technology Asset Management Policy, University Policy Number 3364-65-05.

(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 the university's Information Security and Technology Administrative Safeguards Policy, Policy Number 3364-65-02.

(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 & 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 the university's Device and Workstation Policy, Policy Number 3364-65-06.

(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 the university's Technology Asset Management Policy, Policy Number 3364-65-05.

(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 the university's Technology Asset Management Policy, Policy Number 3364-65-05.

(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.

Approved by:	Policies Superseded by This Policy:
/s/ Sharon L. Gaber, PhD President November 19, 2018 Date *Review/Revision Completed by:* *Vice President, CIO/CTO* *SLT*	Data Center/Data Closet Access Policy 3364-65-10.1 Initial effective date: October 11, 2007 Review/Revision Date: June 8, 2011, July 18, 2014, November 19, 2018 Next review date: November 19, 2021