Name of Policy: Security access safeguards

Policy Number: 3364-65-04

Approving Officer: President

Responsible Agent: Vice President, CIO/CTO

Scope: All University of Toledo organizational units

Effective date: June 27, 2022

Original effective date: November 19, 2018

	New policy proposal		Minor/technical revision of existing policy
X	Major revision of existing policy		Reaffirmation of existing policy

(A) Policy Statement

The confidentiality, integrity, and availability of sensitive data requires the use of reasonable and appropriate logical and technical security controls. The university will secure its technology assets through measures designed to limit access to sensitive data to authorized users. These measures may include logical access controls, identity controls, workstation and server controls, audit logs, and encryption technology.

(B) Purpose

This policy defines logical access controls and technical safeguards and prescribes their use for technology assets that access, create, process, transmit, receive, or destroy sensitive data.

(C) Scope

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, 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. Sensitive data is 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) Access, Identity, and Audit Controls. The university will implement procedures to limit access to Sensitive Data only to authorized users of the data. The requirements for access and identity controls are established under the university's Information Security and Technology Administrative Safeguards Policy, Policy Number 3364-65-02.

(2) Workstation and Device Controls. The logical access control and technology safeguard requirements for Devices and Workstations are established under the university's Device and Workstation Policy, Policy Number 3364-65-06.

(3) Contingency Plans. Procedures for developing contingency plans are established under the university's Information Security and Technology Administrative Safeguards Policy, Policy Number 3364-65-02.

(4) Encryption. Strong encryption, as designated by the Information Security Office and informed by a risk analysis, is the default mechanism to ensure the confidentiality of the contents of a message. Exceptions and alternatives to this requirement may be made by the Information Security Office.

(5) Audit Logs. Access to university technology assets and sensitive data will be logged where possible. The logs will be protected from unauthorized access or modification and they will be retained for an appropriate period of time. Information security office will monitor and review audit logs when an incident occurs to identify and respond to inappropriate activities on a regular basis.

(6) Redistribution of Sensitive Data. A user's rights to access sensitive data does not include the right to move this data or redistribute said data to any other user or organization. No user with the right to access sensitive data may move said data to any asset that is not owned and managed by the University of Toledo. Sensitive data must always reside on University of Toledo own and managed assets that are fully encrypted and meet all regulatory requirements that govern the University of

Toledo.

Approved by: /s/ Gregory C. Postel, M.D. President June 27, 2022_________________ Date *Review/Revision Completed by:* Vice President, CIO/CTO, Senior Leadership Team	**Policies Superseded by This Policy:** • *Access Control Policy 3364-65-02* • *Transmission Control Policy 3364-65-03* • *Remote Access Security Policy 3364-65-11* • *Boundary Security Policy 3364-65-14* • *Password Security Policy 3364-65-07.1* Initial effective date: November 19, 2018 Review/revision date: June 27, 2022 Next review date: June 27, 2025