


<p><b>Name of Policy:</b> Security access safeguards</p> <p><b>Policy Number:</b> 3364-65-04</p> <p><b>Approving Officer:</b> President</p> <p><b>Responsible Agent:</b> Vice President, CIO/CTO</p> <p><b>Scope:</b> All University of Toledo organizational units</p>	<div data-bbox="1166 218 1464 331" style="text-align: right;">  <p>THE UNIVERSITY OF <b>TOLEDO</b> 1872</p> </div> <p><b>Effective date:</b> June 27, 2022</p> <p><b>Original effective date:</b> November 19, 2018</p>				
<table style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 50%; border-bottom: 1px solid black; text-align: center;"> <input type="checkbox"/> New policy proposal         </td> <td style="width: 50%; border-bottom: 1px solid black; text-align: center;"> <input checked="" type="checkbox"/> Minor/technical revision of existing policy         </td> </tr> <tr> <td style="border-bottom: 1px solid black; text-align: center;"> <input type="checkbox"/> Major revision of existing policy         </td> <td style="border-bottom: 1px solid black; text-align: center;"> <input type="checkbox"/> Reaffirmation of existing policy         </td> </tr> </table>		<input type="checkbox"/> New policy proposal	<input checked="" type="checkbox"/> Minor/technical revision of existing policy	<input type="checkbox"/> Major revision of existing policy	<input type="checkbox"/> Reaffirmation of existing policy
<input type="checkbox"/> New policy proposal	<input checked="" type="checkbox"/> Minor/technical revision of existing policy				
<input type="checkbox"/> Major revision of existing policy	<input type="checkbox"/> 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 affiliates, vendor/vendee relationships or other contractual relationships where Sensitive Data 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 sensitive data. Exceptions and alternatives to this requirement must be approved 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.

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 owned and managed assets that are fully encrypted and meet all regulatory requirements that govern the University of

Toledo.

<p>Approved by:</p> <p><u>/s/</u></p> <p>James Holloway, Ph.D. President</p> <p><u>June 27, 2022</u> Date</p> <p><i>Review/Revision Completed by:</i> Vice President, CIO/CTO, Senior Leadership Team</p>	<p><b>Policies Superseded by This Policy:</b></p> <ul style="list-style-type: none"><li>• <i>Access Control Policy 3364-65-02</i></li><li>• <i>Transmission Control Policy 3364-65-03</i></li><li>• <i>Remote Access Security Policy 3364-65-11</i></li><li>• <i>Boundary Security Policy 3364-65-14</i></li><li>• <i>Password Security Policy 3364-65-07.1</i></li></ul> <p>Initial effective date: November 19, 2018</p> <p>Review/revision date: June 27, 2022, July 16, 2025</p> <p>Next review date: June 27, 2025</p>
---	---