


<p>Name of Policy: Security Access Safeguards</p> <p>Policy Number: 3364-65-04</p> <p>Approving Officer: President</p> <p>Responsible Agent: Vice President, CIO/CTO</p> <p>Scope: All University organizational units</p>	 <p>Original Effective Date: November 19, 2018</p>				
<table> <tr> <td><input checked="" type="checkbox"/> New policy proposal</td> <td><input type="checkbox"/> Minor/technical revision of existing policy</td> </tr> <tr> <td><input type="checkbox"/> Major revision of existing policy</td> <td><input type="checkbox"/> Reaffirmation of existing policy</td> </tr> </table>		<input checked="" type="checkbox"/> New policy proposal	<input type="checkbox"/> Minor/technical revision of existing policy	<input type="checkbox"/> Major revision of existing policy	<input type="checkbox"/> Reaffirmation of existing policy
<input checked="" type="checkbox"/> New policy proposal	<input 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 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 based on an appropriate risk analysis.
 - (5) Audit Logs. Access to university technology assets and sensitive data will be logged. 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 to identify and respond to inappropriate activities on a regular basis.

<p>Approved by:</p> <p><u>/s/</u> Sharon L. Gaber, PhD President</p> <p><u>November 19, 2018</u> Date</p> <p><i>Review/Revision Completed by:</i> <i>Vice President, CIO/CTO</i> <i>SLT</i></p>	<p>Policies superseded by this policy:</p> <p>Access Control Policy, formerly Policy No. 3364-65-02</p> <p>Transmission Control Policy, formerly Policy No. 3364-65-03</p> <p>Remote Access Security Policy 3364-65-11 Boundary Security Policy 3364-65-14 Password Security Policy 3364-65-07.1</p> <p>Initial effective date: November 19, 2018</p> <p>Review/Revision Date: N/A</p> <p>Next review date: November 19, 2021</p>
---	---