3364-65-04 Security access safeguards.

(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 rule 3364-65-05 (technology asset management).

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

(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 rule 3364-65-05 (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) 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 rule 3364-65-02 of the Administrative Code (information security and technology administrative safeguards).

(2) Workstation and device controls. The logical access control and technology safeguard requirements for devices and workstations are established under rule 3364-65-06 of the Administrative Code (device and workstation policy).

(3) Contingency plans. Procedures for developing contingency plans are established under rule 3364-65-02 of the Administrative Code (information security and technology administrative safeguards).

(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.

Effective: 3/11/2019

CERTIFIED ELECTRONICALLY

Certification

03/01/2019

Date

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