Ohio Administrative Code

Rule 3341-6-64 Information Security.

Effective: July 16, 2026

(A) Policy statement and purpose

This policy serves as a measure to protect the confidentiality, integrity, and availability of institutional data as well as any information systems that store, process, or transmit institutional data. This policy establishes a framework to safeguard the university's electronic information resources and computing and networking infrastructure from threats and to ensure compliance with applicable laws and regulations.

(B) Policy scope

This policy applies to all faculty, staff, students, third-party agents, contractors, and any other university affiliates authorized to access institutional data or use university-owned information systems. It encompasses all data and systems owned, managed, or used by the university, regardless of where they are stored or accessed.

(C) Policy definitions

(1) Institutional data

Data that are created, collected, stored, or managed by the university in the course of its academic, research, or administrative operations, including but not limited to student records, financial data, employee information, and research data.

(2) Information systems

Any hardware, software, networks, or services used to store, process, or transmit institutional data, including university-owned devices, cloud services, and personal devices used for university business.

(3) Principle of least privilege

The principle of least privilege is a foundational aspect of information security. It states that people should only have access to the minimum amount of data and systems that they require to perform the specific, intended functions of their jobs.

(4) University affiliate

Any individual or entity authorized to access institutional data or information systems, including faculty, staff, students, contractors, vendors, and third-party agents.

(D) Policy

BGSU is committed to protecting the confidentiality, integrity, and availability of its institutional data and information systems. The university adopts the following principles to achieve this objective:

(1) Data protection

All institutional data must be protected in accordance with its classification, as defined by the university's data use and protection policy.

(2) System security

Information systems must be configured, maintained, and operated in a manner that minimizes risks to their security and ensures their availability for authorized use, as defined in the documentation and procedures approved by the information security office, given the level of classification, value and criticality that the system and its data have to the university.

(3) User responsibility

All university affiliates are responsible for safeguarding institutional data and information systems they access or use, adhering to university policies, procedures, and guidelines as defined by the information security office.

(4) Risk management

The university will implement risk-based security measures (applying the principle of least privilege) to identify, assess, and mitigate threats to institutional data and information systems.

(5) Legal and contractual compliance required

All activities involving institutional data and information systems must comply with federal, state, and local laws, as well as university policies and contractual obligations.

(E) Roles and responsibilities

(1) Information security office (ISO)

The BGSU information security office, under the direction of the director of information security, is responsible for:

(a) Developing, maintaining, and enforcing this policy and related guidelines.

(b) Conducting risk assessments and security audits.

(c) Providing training and awareness programs for university affiliates.

(d) Responding to security incidents and coordinating remediation efforts.

(e) Reviewing this policy annually, and more frequently if necessary, due to changes in technology, regulatory requirements, or university operations.

(2) University affiliates

University affiliates must:

(a) Comply with this policy and related security guidelines, including the ITS security standards.

(b) Report suspected security incidents to the ISO immediately. To report a security incident, contact:

Email: infosec@bgsu.edu BGSU information security office office of information technology services 419-372-0999

(c) Complete mandatory security awareness training as required.

(3) University administration - all divisions

University administrators must ensure that their units comply with this policy and allocate resources to support security measures. In addition to being key stakeholders, university administrators are responsible for understanding the security risks that are associated with the decisions being made in their areas regarding institutional data and information systems. This responsibility includes collaborating with the ISO to ensure they are aware of these risks.

(4) Vendors and contractors

Vendors and contractors must adhere to this policy and any additional security requirements specified in their contracts with the university.

(F) Compliance and enforcement

The ISO will investigate reported violations and recommend appropriate sanctions to the relevant university decisional authority (e.g., office of human resources, office of the provost, or office of the dean of students).

Violations of this policy may result in disciplinary action, including but not limited to:

(1) Suspension or loss of access privileges to institutional data or information systems.

(2) Sanctions for employees, up to and including termination of employment.

(3) Sanctions for students in accordance with the student code of conduct.

(4) Sanctions for vendors and contractors, up to and including termination for default and loss of status as an active supplier.

(5) Legal action, where violations involve criminal activity.

(G) Exceptions

Any requests for exceptions to this policy must follow the formal exception procedure as defined by the BGSU IT security standards exception procedure.

(H) Related policies

3341-6-07 Acceptable uses of BGSU information technology.

3341-6-18 Data use and protection.

3341-6-62 Password standards.