THE OHIO STATE UNIVERSITY

Information Technology (IT) Security

University Policy

Applies to: Faculty, staff, and students, academic and administrative units, affiliated entities, agents, suppliers/contractors, and volunteers

Responsible Office

Office of the Chief Information Officer

POLICY

Issued: 08/18/2010
Revised: 03/01/2011
Edited: 12/16/2021

This policy provides guidance for establishing information technology (IT) security requirements for all **information assets** and systems under the university's defined control and for the personnel who access these systems.

Adherence to these requirements ensures that the university protects its information assets with due diligence, complies with government regulatory and contractual requirements, and meets industry best practices for this protection.

Purpose of the Policy

To provide guidance for establishing IT security requirements.

Definitions

Term	Definition
Data	Groups of information that represent attributes of variables stored, transmitted, and/or processed by IT.
Information asset	A definable piece of information recognized as having value to the university.
Malicious code	A computer program that causes undesirable results.
Threats	The danger of attack on one or more systems assets.
Security policies	A statement or statements of how the university intends to protect information and systems assets.
Standards, requirements, guidelines, and practices	Standards, requirements, guidelines, and practices are operable realizations of security policies.
Senior leadership	The highest managerial level within the university, for example the provost, president, CEO of the Wexner Medical Center, Senior Management Council, President's Cabinet, etc.
Systems assets	Information technology software and/or hardware used in conjunction with information assets to fulfill university needs. This includes telecommunication and mobile computer systems.

Policy Details

I. The university must provide its faculty, students, and staff (to include contractors or other authorized agents with access to university IT resources, **data**, or assets) with clear direction for the safeguarding of university information assets.

II. This IT Security policy establishes the overall intent of the organization to support and promote information security in all its practices.

III. Statements created to support particular elements of the information security practice at the university will be organized into existing policies, **standards, requirements, guidelines, and practices**. Creation of new policies, standards, requirements, guidelines, and practices to support the intent of this policy is allowed.

IV. The Office of the Chief Information Officer or its appointed designees will manage the IT Security policy and its derivative works.

V. University organizations (e.g., colleges, vice presidential units) will be solicited to designate a security representative as the local organizational contact to be the liaison with the chief information security officer's group for security related matters.

VI. Scope
   A. This policy applies to all colleges and units established by the university that exercise any IT function relating to the mission of the university except for those specifically exempted in writing by the **senior leadership** of the university.
   B. This policy applies to university computer and telecommunications systems; faculty, staff, and students; academic and administrative units; affiliated entities, agents, contractors, and volunteers of the university who use and/or administer such systems.

VII. Rationale
   A. The ability for the university to meet the daily needs of the academic, administrative, and research communities is facilitated, in large part, through the use of IT. This technology allows faculty, staff, and students to meet their diverse requirements (e.g., collaboration, research, communication, etc.). While critical to the business of the university, these technologies also introduce risks. The risks and corresponding **threats** associated with IT are increasing in both number and variety. Information technology infrastructures are increasingly complex to implement and administer. The advent of hacking tools and persons willing to distribute viruses and **malicious code** have increased the risks to IT organizations and the assets they are charged to safeguard.
   B. University mission-critical functions supported by IT systems continue to expand. Although some data and systems may not be classified as mission critical, they nevertheless represent a significant investment in resources, may contain sensitive data, and are efficient methods of providing a wide range of education-related services. Coupled with overall system integration and interconnectivity, university systems and networks are increasingly at risk to intrusions, misuse of data, and other attacks from both internal and external sources.
   C. A successful security framework is reliant upon strong leadership support and a comprehensive body of effective and efficient IT security standards and procedures that:
      1. Promote public trust,
      2. Ensure continuity of services,
      3. Comply with legal and contractual requirements,
      4. Recognize risks and threats, and
      5. Protect **systems assets**.

VIII. Enforcement
   A. Failure to comply with this policy may result in suspension of access to information assets and information systems or both and may also result in disciplinary action, up to and including termination and criminal prosecution.

PROCEDURE

Issued: 08/18/2010
Revised: 03/01/2011
Edited: 12/16/2021

I. The university, as part of an overall security management strategy, shall develop IT **security policies**, standards, requirements, guidelines, and practices in support of the university "Information Security Framework". All IT security policies, standards, requirements, guidelines, and practices shall ensure compliance with all federal and state security-related regulations that apply to the university's mission and services. These instruments shall

consider organizational risk and business impact within their design and be written to recognize the resource impact and constraints of university organizations.

II. The university shall ensure that faculty, staff, students, and any university partners are aware of their specific information security responsibilities in the use of information systems and the handling of information assets.

III. The Information Security Standard (ISS) and the Information Security Control Requirements (ISCR) establish the university's minimum security requirements and provide the foundation for IT security policy development. The core assumptions of these requirements are adapted from the National Institute of Standards and Technology (NIST) Risk Management Framework and Security Controls.

A. Risk Management: The university shall apply risk management techniques to balance the need for security measures considering the cost benefit analysis to make informed decisions and to aid in designing and implementing any security policies, standards, requirements, guidelines, and practices. Impact upon the teaching, research, and service mission of the university will be considered as a key factor in this process.

B. Confidentiality, Integrity and Availability: The university shall ensure that its IT security policies, standards, requirements, guidelines, and practices address the basic security elements of confidentiality, integrity, and availability.

C. Protection, Detection, and Response: Security policies, standards, requirements, guidelines, and practices shall include methods to protect against, detect, and respond to threats and vulnerabilities to unit information and systems. These instruments will be implemented with consideration of business impact and resource constraints for all university units tasked with their implementation.

D. Identification and Authentication: The university shall implement identification and authentication requirements for information systems and services that protect the university's data and physical IT resources in the most appropriate manner.

E. Access Control and Authorization: The university shall implement access control and authorization policies, plans, standards, and procedures required to protect system assets and other information resources maintained by its colleges and offices.

F. Security Audit Logging: The university shall implement a security audit logging capability for information systems, including computers and network devices.

G. Security Management and Administration: The university shall implement a university-wide security management and administration program.

H. Process Management: Standards, requirements, guidelines, and practices created to support this overarching IT Security policy must be reviewed and made available to university committees and appointed security representatives of the university technical, faculty, and general user communities before being put into place. These reviewing organizations must be explicitly enumerated in the draft of each process management document. The assigned groups will vary based upon the subject matter of the document but must include at least one body from the above general categories before the adoption of the policy, standard, requirement, guideline, or practice. Instruments designed through this process will be reviewed and revised using the timeline established for university policy review.

Responsibilities

Position or Office	Responsibilities
Office of the Chief Information Officer	1. Coordinate and administer the IT security program. 2. Develop and maintain security policies, standards, requirements, guidelines, and practices to ensure information security and the associated action steps to prevent and mitigate fraud. 3. Develop and maintain appropriate training and associated reporting. 4. Periodically review and update the IT security program. 5. Provide an annual report on the program effectiveness. 6. Direct creation of instruments (standards, requirements, guidelines, and practices) on specific technical subjects or in specific areas of security concern to support the intent of this policy.

Applies to: Faculty, staff, and students, academic and administrative units, affiliated entities, agents, suppliers/contractors, and volunteers

Position or Office	Responsibilities
Colleges, VP units, and regional campuses	1. Review internal processes; implement standards, requirements, guidelines, and practices as necessary. 2. Update internal control structure or standard operating procedures as appropriate to reflect university guidelines. 3. Annually review internal processes, control structures, and standard operating procedures for continued compliance with policies, standards, requirements, guidelines, and practices. 4. Provide impact assessment and feedback on standards, guidelines, requirements, and practices governed by this policy. 5. Identify who must complete training and ensure that training is completed. 6. Protect identifying information collected in accordance with all university policies. 7. Report proven or suspected disclosure or exposure of personal information in accordance with the Information Security Response Management policy.
All individuals to whom this policy applies	1. Follow documented internal processes. 2. Provide impact assessment and feedback on standards, guidelines, requirements, and practices governed by this policy. 3. Complete university required security training. 4. Report proven or suspected disclosure or exposure of personal information, financial fraud, suspected, or actual identity theft to supervisor immediately.

Resources

University Policies, policies.osu.edu
- Identity Theft Red Flags, busfin.osu.edu/sites/default/files/516_identitytheftredflags.pdf
- Information Security Incident Response Management, go.osu.edu/infosec-isirmp
- Institutional Data, go.osu.edu/idp
- Payment Card Compliance, busfin.osu.edu/sites/default/files/515_creditcard.pdf
- Public Records, compliance.osu.edu/PublicRecordsPolicy.pdf
- Responsible Use of University Computing and Network Resources, go.osu.edu/rup

Information Security Standards and Requirements
- Information Security Control Requirements (ISCR), go.osu.edu/infosec-iscr
- Information Security Standard (ISS), go.osu.edu/infosec-iss

Other
- National Institute of Standards and Technology (NIST) Risk Management Framework, csrc.nist.gov/groups/SMA/fisma/framework.html

Contacts

Subject	Office	Telephone	E-mail/URL
Policy questions	Office of the Chief Information Officer, Chief Information Security Officer	614-292-7831	riskmgmt@osu.edu ocio.osu.edu/itsecurity

History

Issued:	08/18/2010	As Interim
Revised:	03/01/2011	
Edited:	05/13/2011	
Edited:	07/11/2011	
Reviewed:	05/06/2015	
Edited:	06/29/2015	

Applies to: Faculty, staff, and students, academic and administrative units, affiliated entities, agents, suppliers/contractors, and volunteers

Reviewed: 05/16/2016
Edited: 12/16/2021