Information Technology (IT) Security 1.1.40

College Policy

Applies to: Faculty, staff, students, affiliated entities, suppliers/contractors and volunteers.

Responsible Office **Office of the President**

POLICY STATEMENT

This policy provides guidance for establishing Information Technology (IT) security requirements for all **information assets** and systems that are owned by Central Ohio Technical College (COTC) and for the personnel who access these systems.

Adherence to these requirements ensures that COTC 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 assets	A definable piece of information recognized as having value to the college.
Malicious code	A computer program that causes undesirable results.
Threats	The danger of attack on one or more system assets.
The Office of Technology and Digital Innovation (OTDI)	The OTDI provides Information Technology (IT) services to Central Ohio Technical College (COTC).
Security policies	A statement or statements of how the college intends to protect information and systems assets.
Standards, requirements, guidelines, and practices	Standards, requirements, guidelines, and practices are operable realizations of security policies.
System assets	Information Technology software and/or hardware used in conjunction with information assets to fulfill college related needs. This includes telecommunication and mobile computer systems.

Policy Details

I. COTC must provide its faculty, staff and students (to include contractors or other authorized vendors with access to college information technology resources, **data** or assets) with clear direction for the safeguarding of college information assets.

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

III. Statements created to support various elements of these information security practices at COTC 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 permitted.

IV. The Office of Technology and Digital Innovation (OTDI), The Ohio State University, in partnership with COTC, will manage the IT Security policy and its derivative works.

Information Technology (IT) Security 1.1.40

College Policy

Applies to: Faculty, staff, students, affiliated entities, suppliers/contractors and volunteers.

V. Rationale

A. The ability for the college to meet the daily needs of the academic and administrative support areas is facilitated, in large part, using IT. This technology allows faculty, staff and students to meet the diverse requirements that take place within the institution. While critical to the mission of the college, these technologies also introduce risks. The risks and corresponding **threats** associated with IT are increasing in both number and variety. IT 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. College 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, college 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 information technology security standards and procedures that:

i. Promote public trust
ii. Ensure continuity of services
iii. Comply with legal and contractual requirements
iv. Recognize risks and threats
v. Protect system assets

VI. Enforcement

Failure to comply with these policies 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

I. COTC in partnership with the OTDI, as part of the college's overall security management strategy, shall develop an IT Security policy and associated security standards, guidelines, requirements and practices in support of the college's "Information Security Program." This IT Security policy and supporting standards, guidelines, requirements and practices shall ensure compliance with all federal and state security-related regulations that apply to the college's mission and services. These instruments shall consider organizational risk and business impact, and be written to recognize the resource impact and constraints of college organizations.

II. COTC will promote awareness to faculty, staff, students and any associated contractors/vendors of their specific information security responsibilities in the use of information systems and the handling of information assets.

III. COTC will follow Ohio State University's Information Security Standard (ISS) and the Information Security Control Requirements (ISCR) with limited exceptions. The core assumptions of these requirements are adapted from the National Institute of Standards and Technology (NIST) Risk Management Framework and Security.

A. Risk Management: The OTDI, in partnership with COTC, 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 standards, guidelines, requirements and practices with the mission and goals of the institution. The academic service mission of the college will be considered as a key factor in this process.

Applies to: Faculty, staff, students, affiliated entities, suppliers/contractors and volunteers.

B. Confidentiality, Integrity and Availability: COTC shall ensure that the IT Security policy and standards, guidelines, requirements and practices address the basic security elements of confidentiality, integrity and availability.

C. Protect, Detect, and Respond: This policy and the associated security standards, guidelines, requirements and practices shall include methods to protect against, detect, and respond to threats and vulnerabilities to college information and system assets. These instruments will be implemented with consideration of business impact and resource constraints for all college areas tasked with their implementation.

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

E. Access Control and Authorization: COTC, in partnership with the OTDI, shall implement access control and authorization procedures that protect IT system assets and other information resources maintained by the college and its offices.

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

G. Security Management: COTC, in partnership with the OTDI, shall implement a college-wide security management program.

H. Process Management: The IT Security policy and supporting standards, guidelines, requirements, and practices will be incorporated into the various business and academic processes that take place throughout the college. This will be done to ensure the security of IT system assets and information, while allowing for effective processes to take place in support of the college's mission and goals.

Responsibilities

Position or Office	Responsibilities
Office of Technology and Digital Innovation (OTDI), The Ohio State University	1) Coordinate the IT Security Program. 2) Assist in the development and maintenance of the IT Security policy and associated security standards to ensure information security and the associated action steps to prevent and mitigate fraud. 3) Periodically review and update the IT security program. 4) Lead annual check-in with COTC leadership. 5) Provide an annual report on the program effectiveness. 6) Create security practices and training on specific technical subjects or in specific areas of security concern to support the intent of this policy. 7) Annually distribute training materials to COTC faculty and staff.
College departments	1) Review internal processes and confirm that appropriate security practices in accordance with this security policy and standards, guidelines, requirements and practices are being adhered to. 2) Update internal control structures or standard operating procedures as appropriate to reflect the security practices and guidelines provided in this policy and the associated security standards, guidelines, requirements and practices. 3) On an as-needed basis, review internal processes, control structures and standard operating procedures for continued compliance with the guidelines provided in this policy and the associated security standards, guidelines, requirements and practices. 4) Provide impact assessment and feedback on the security standards, guidelines, requirements and practices governed by this policy. 5) Protect identifying information collected in accordance with all college policies. 6) Report proven or suspected disclosure or exposure of personal information to the OTDI Digital Security and Trust team.
Individuals to whom this policy applies	1) Follow documented internal processes.

Information Technology (IT) Security 1.1.40

College Policy

Applies to: Faculty, staff, students, affiliated entities, suppliers/contractors and volunteers.

Position or Office	Responsibilities
	2) Provide impact assessment and feedback on standards, guidelines and practices governed by this policy and associated security standards. 3) Review college provided security training materials. 4) Report proven or suspected disclosure or exposure of personal information, financial fraud, and suspected or actual identity theft to your supervisor immediately.

Resources

Responsible Use of Computing and Network Resources Policy
National Institute of Standards and Technology (NIST) Risk Management Framework, csrc.nist.gov/groups/SMA/fisma/framework.html
The Ohio State University Information Security Standards
The Ohio State University Information Security Controls Requirements

Contacts

Subject	Office	Telephone	E-mail/URL
Policy Questions	Information Technology Services Dept, The Office of Technology and Digital Innovation, The Ohio State University	740-366-9244	NWK-helpdesk@osu.edu
Incidents of proven or suspected disclosure or exposure of personal information	Digital Security and Trust, The Office of Technology and Digital Innovation, The Ohio State University	740-366-9244	security@osu.edu

History

Issued: March 9, 2023 (Initial draft available October 1, 2012)