



Ohio Administrative Code

Rule 3362-5-30 Campus computer and network use.

Effective: July 1, 2024

(A) Purpose and application

(1) This policy outlines the guidelines for responsible management and security of Shawnee state university's (SSU) digital resources, ensuring alignment with relevant procedures (SSU information security program and conditions for use), and compliance with applicable regulatory frameworks. It is designed to protect the integrity, confidentiality, security, and availability of SSU's technology services and applies to all individuals interacting with SSU's digital and network resources.

(2) Universal in scope, this policy encompasses both on-campus and remote interactions with SSU's technology resources, covering all affiliated and non-affiliated individuals.

(B) Responsibilities and authority

(1) All users are required to comply with this policy, its applicable procedures (SSU information security program and conditions for use), and relevant legal and regulatory standards.

(2) The chief information security officer (CISO) is tasked with the oversight of this policy, ensuring its ongoing relevance, compliance with legal and operational standards, and the implementation of requisite security measures.

(C) Access privileges and restrictions of use

Access to digital resources is predicated on authenticated identity and relevant authorizations, managed in accordance with the SSU information security program and conditions of use procedures.

(D) Privacy expectations



(1) Users should anticipate monitoring of university technology resources, in adherence to the information security program and conditions of use procedures for operational and security purposes.

(2) SSU commits to protecting sensitive information in accordance with Family Educational Rights and Privacy Act (FERPA), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), and other regulations, as outlined in the information security program procedure.

(E) Use of university computing resources

(1) Adherence to the information security program and the conditions for use procedures is mandatory in order for users to be granted the privilege of access to the university's information technology systems.

(2) All users are responsible for complying with the information security program and the conditions for use procedures when accessing university resources, and networks. The information security program and the conditions for use procedures shall be posted on the university policies and the information technology services web pages and made available upon request.

(F) Sanctions

Violations of this policy and applicable procedures will be subject to discipline according to university policies and collective bargaining agreements.