3362-5-30 Campus computer and network use.

(A) Purpose and application

(1) The purpose of this rule is to establish the obligations of users and managers of university-provided technologies and related resources. All users and managers of university-provided and supported information technologies are required to abide by applicable federal and state laws, relevant regulations, conditions for use, and best practices to ensure the highest level of confidentiality, integrity, security, and availability of technology services that can be afforded by the university.

(2) This rule applies to all users of campus computing and network resources, whether or not employed by or affiliated with the university, and for all uses of computing and network resources whether on campus or from remote locations.

(B) Responsibilities and authority

(1) All users are responsible for complying with this rule, conditions for use, and any laws or regulations applicable to computer systems, information security, network access, and application computing.

(2) The university's chief information officer (CIO) is responsible to maintain applicable policies and to ensure the conditions for use reflect current operational expectations, incorporate best practices and technical updates, and to implement measures required for compliance with applicable laws and regulations that ensure privacy and security of data and delivery of appropriate access to network resources.

(C) Access privileges and restrictions of use

(1) Access privileges are contingent upon the authentication of an

identity and authorization of that identity to access specific technologies required to fulfill assigned roles or to complete the applications and activities of that identity at the university. Such access depends upon the role assigned by the department of human resources upon employment or contractual relationship with the university. Additional accesses may be managed by department supervisors in accordance with university policies.

(2) Use of the university's computing systems, resources and networks (on-site and remote) is granted solely to Shawnee state active employees and retirees with ten years of continuous service, currently enrolled students, contractual and term employees, and others who have a business or operational need for access and are designated in writing by the president or vice president for finance and administration. The university will adopt measures necessary to protect its computing systems and network including implementation of multi-factor authentication.

(3) Commercial use of the university's computing systems, resources, and networks is prohibited without prior written consent from the office of the General Counsel

(4) Once on-site and remote access to technology systems is assigned in accordance with human resources policies, any modification of that access that involves personal and shared data may be extended to or retracted from the initial authorized account users with written consent of the respective vice president and in accordance with human resource and relevant university policies.

(5) The university reserves the right to limit, restrict, extend or deny computing privileges and access to its resources.

(6) Testing and monitoring of security will be routinely conducted as well as the regular review of files or information resident on university systems to guard against unacceptable use. All accounts assigned to authorized individuals will be treated as private by university employees charged with managing university computer systems, resources, and networks.

(7) An account may be accessed without the user's permission by the appropriately assigned ITS officials upon authorization by the

president or the president's designee for any employee placed on temporary or extended leave of absence, or otherwise is not reasonably available, or when there is probable suspicion of violation of university policies or evidence of criminal activity. The university reserves the right to deny access to its computer systems, resources and networks until consent to access the account is provided by the president or president's designee.

(D) Privacy expectations

(1) Users are expected to be aware that their uses of university computing systems, resources, and networks are not private. The university routinely monitors individual and campus-wide usage on a regular basis for suspicious activity and targeted threats. Service vendors often require the examination of institutional files, data transmissions, and system-generated logging files to maintain normal operations.

(2) Shawnee state's status as a financial institution obligates the university to protect the consumer information it collects during the normal course of business. Users authorized to maintain financial information must adhere to all state and federal mandates and compliance required to meet external or internal audit requirements.

(3) As an institution of higher education, Shawnee state is obligated to protect confidential information restricted by FERPA, HIPAA, GLBA, GDPR, PCI, Ohio revised code and other regulatory requirements (e.g. red flag rules), and is not releasable to the public under state or federal law.

(E) Use of university computing resources

(1) Adherence to the conditions for use 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 conditions for use of Shawnee state's computer systems, resources, and networks. conditions for use shall be distributed to users via e-mail when substantive modifications are adopted. They shall be posted on the university information services web page and made available upon

request.

(3) As a member of the Ohio academic research network (OARnet), Shawnee state is expected to ensure compliance with policies and procedures of OARnet and related networks. Therefore, users granted privileges to access OARnet and other networks must comply with the policies and procedures of those networks.

(F) Sanctions

(1) Violation of computer use policies or non-adherence to the conditions for use may result in sanctions by the university, up to and including loss of computing privileges, termination of employment and dismissal from the university in accordance with the appropriate policies and collective bargaining agreements regarding disciplinary actions.

(2) The process outlined in the student handbook will determine sanctions for students.

(3) Disciplinary actions do not preclude additional civil or criminal prosecution by the appropriate authority.

Effective: 3/26/2020

CERTIFIED ELECTRONICALLY

Certification

03/16/2020

Date

Promulgated Under:	111.15
Statutory Authority:	3362.03
Rule Amplifies:	3362.03