RESOLUTION F10-24

APPROVAL TO ADOPT POLICY 5.30REV
DIGITAL RESOURCE MANAGEMENT & SECURITY

WHEREAS, an ongoing review of institutional policies has been undertaken in order to remove outdated policies, and to modify and update policies to ensure their accuracy and application to current organizational needs and regulatory requirements; and

WHEREAS, Policy 5.30Rev., Campus Computer and Network Use, was last reviewed and approved by the Board of Trustees on March 13, 2020; and

WHEREAS, the University is committed to managing its digital resources and 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 Standards (PCI DSS) and other regulations; and

WHEREAS, a modification of the policy and the adoption of an information security procedure is warranted to comply with federal mandates and establish guidelines for the responsible management and security of the University's digital resources; and

WHEREAS, the proposed policy is renamed "Digital Resource Management & Security"; and

WHEREAS, these revisions have been recommended by the President for Board of Trustees approval; and

NOW, THEREFORE, IT IS RESOLVED that the Board of Trustees of Shawnee State University approves revisions to former Policy 5.30Rev., Campus Computer and Network Use, and renames the policy Digital Resource Management & Security.

(June 21, 2024)

Shawnee State University

1.0   PURPOSE AND APPLICATION

1.1   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.

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

2.0   RESPONSIBILITIES AND AUTHORITY

2.1   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.

2.2   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.

3.0   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*.

4.0   PRIVACY EXPECTATIONS

    4.1   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.

    4.2   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*.

5.0   USE OF UNIVERSITY COMPUTING RESOURCES

    5.1   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.

    5.2   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.

6.0   SANCTIONS

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

History:
Effective: 9/11/2001
Revised: 06/21/2024; 03/13/2020; 02/09/2007

Applicable Procedures: 5.30:1 Conditions for Use
                              5.30:2 Information Security Program