Policy: Technology Acceptable Use Policy

Policy Details

Revised: Nov. 1, 2024

Author(s): Heather De La Cruz, Security Analyst
Joshua Rhoden, Director of Infrastructure and Security
Neal Dyer, Chief Technology Officer

Effective: Nov. 1, 2024

Introduction:

Southeastern University's (SEU) Department of Information Technology (IT) is committed to providing the community, including staff, faculty, students, and partners, with robust and secure information systems, networks, and other resources. This includes protecting the community from illegal or damaging actions by individuals, either knowingly or unknowingly.

Purpose:

To identify acceptable and unacceptable usage of SEU's information systems, network, and data.

Scope:

All information assets, including, but not limited to, data, information systems' hardware and software, and network communications, both owned and leased by SEU.

Policy:

General Use and Ownership

All personnel accessing SEU information systems are required to adhere to the following guidelines:

- Data Protection: Ensure proprietary information is protected in accordance with applicable regulations, including FERPA, GLBA, HIPAA, and related standards.
- Incident Reporting: Promptly report theft, loss, or unauthorized disclosure of SEU proprietary information to IT Security at security@seu.edu.
- System Auditing: SEU reserves the right to audit its networks and systems. The Department of Information Technology may monitor any data stored or transmitted on SEU systems.
- Cloud Storage:
    - Cloud storage services (Google Drive, OneDrive) are provided for official SEU business purposes.
    - SEU is not responsible for personal data stored on these platforms.
    - SEU email, cloud storage, and other IT resources will be deactivated immediately upon termination of employment, 60 days from graduation, or after three semesters of inactivity.
- Email Use:
    - SEU email should be used only for official SEU-related purposes.
    - SEU is not obligated to deliver personal emails upon an employee's resignation or termination.
- Privacy Expectation: Users should not expect privacy for anything stored, sent, or received on SEU-managed systems.
- Mass Emails: Mass emails (emails sent to the majority population of SEU) may only be sent with prior approval by IT and the office of the President.
- Workstation Security: Ensure computer screens are locked or the user is logged off when away from their workstation.
- Personal Data: SEU systems are intended for official use, and SEU is not responsible for personal data transmitted or stored.

Acceptable Use

The acceptable use of SEU's information systems is aligned with the university's mission to support academic, research, and business functions. Users are expected to:

- Use SEU-provided systems and data for legitimate educational, business, or research purposes.
- Follow all applicable laws and university policies regarding the use and protection of data and technology resources.
- Report any suspicious activity, data breaches, or security incidents immediately to IT Security.

Unacceptable Use

The following activities are prohibited on SEU's information systems:

- Data & Information:
    - Unauthorized disclosure of SEU proprietary information or Personally Identifiable Information (PII) to unauthorized individuals, systems, or AI models.
    - Duplicating copyrighted materials (e.g., images, music, software) without proper authorization or licensing.
    - Accessing SEU data, servers, or systems for non-academic or non-business purposes.
- Security & Malicious Activity:
    - Introducing malicious code (e.g., viruses, worms, crypto-malware) into SEU's systems or networks.
    - Exporting software or technology in violation of export laws.
    - Sharing passwords or service account credentials outside of SEU's managed password system.
    - Engaging in activities that violate sexual harassment or hostile workplace laws via SEU systems.
    - Accessing inappropriate content as defined by the SEU student handbook (pg. 18, section 4).
- Network & System Abuse:
    - Unauthorized network monitoring, including network sniffing, packet spoofing, and denial of service attacks.
    - Circumventing user authentication or security measures of any SEU systems or networks.
    - Introducing unauthorized technology, such as honeypots or honeynets, onto SEU's network.
    - Tampering with or damaging SEU-owned or leased equipment. Individuals responsible for damage may be required to reimburse SEU for repairs or replacements.
- Other Prohibited Actions:
    - Connecting unauthorized systems to SEU's production network.
    - Installing software not approved by IT.
    - Tampering with or circumventing IT security controls.
    - Providing unauthorized access to SEU information systems.
    - Moving or disconnecting IT equipment (e.g., wireless access points) without approval.

Responsibility:

Individual Accountability

- All personnel accessing the information systems are responsible for adhering to acceptable use conduct of the University's information systems.
- Department of Information Technology
- The Department of Information Technology enforces and audits usage controls on SEU's information systems.

Revision History

Date	Description of Change	Revised by	Approved by