Acceptable Use of Information Technology Resources

Issued 1/25/2024

Version 65

Purpose

This policy defines the acceptable use of Salem State University's (SSU) applications, hardware, digital information and other information technology resources and systems.

Scope

This policy applies to any person utilizing SSU's information technology resources. The following persons are authorized to use SSU information technology resources: (1) current faculty; (2) current staff; (3) current students; and (4) authorized visitors. This policy also applies to the devices they use to connect to SSU resources.

Policy

Acceptable use of SSU information technology resources includes usage for academic, educational or professional purposes which are directly related to official SSU business and in support of SSU's mission. Accordingly, users are encouraged to utilize SSU's information technology resources to the fullest extent in pursuit of the University's mission, goals, and objectives. The University expects that these information technology resources are always utilized in a responsible manner and reserves the right to limit or remove access as needed.

SSU's electronic communications systems, including Internet, telephony, email, and messaging services, are to be used primarily for university-related purposes. Users shall have no expectation of privacy over any communication, transmission, or work performed using or stored on SSU's information technology resources. The University reserves the right to monitor any and all aspects of its information technology resources and to do so at any time, without notice, and without the user's permission. SSU makes no warranties, expressed or implied, for the information technology resources it is providing. SSU will not be responsible for any damages a user may suffer, including loss of data, undelivered messages or content, or service interruptions. SSU denies any responsibility for the accuracy or quality of information obtained through its information technology resources.

Unacceptable use of the SSU electronic communications systems includes, but is not limited to, the following:

- Activities that violate local, state, or federal laws and/or regulations including the use of unlicensed software;
- Excessive, unreasonable, or unauthorized personal use;
- Storing, sending, or forwarding e-mails that contain libelous, defamatory, obscene, inflammatory, threatening, or harassing content;
- Infringing on intellectual property rights;
- Commercial purposes;
- Activities that attempt to circumvent or disable protection mechanisms that have been put in place by SSU

Use of Technology

I. Access

Users of SSU's information technology resources are authorized to access only systems,including hardware and software, where access has been approved, per the *Access Control Policy.*

II. Remote Access

Remote access is authorized for only those users with an approved business or academic use. Users who have been approved for remote access are responsible for adhering to the requirements defined in the SSU *Remote Access Policy.*

III. Media

Users shall not use media, such as flash drives or portable hard drives, until they have been scanned for malware threats to the security or functionality of SSU information technology resources.

IV. Data Encryption and Storage

Confidential and/or personally identifiable information (PII) must be protected by encryption. Encryption methods that have been approved and are listed in the SSU *Encryption Policy* should be utilized in these cases. Users who are

unfamiliar with using approved encryption technologies should seek guidance from the SSU Helpdesk.

V. Cloud Computing and Storage

Advances in cloud computing offer convenient technology solutions such as data storage and connectivity. Data placed on any cloud computing storage solution must adhere to the same policies as data stored on SSU's internal technology resources.

Computer Virus and Malware Protection

It is important that users take particular care to avoid compromising the security of the SSU network. Users shall exercise reasonable precautions in order to prevent the introduction of a computer virus or other malware into the SSU network. Virus scanning software is installed on all SSU systems and is used to check any software downloaded from the Internet or obtained from any questionable source. Users are prohibited from disabling, or attempting to disable, virus scanning software. Users must scan portable media devices for viruses and malware before using them to ensure that they have not been infected. If users are unsure of how to utilize virus and malware scanning tools, they should contact the SSU Helpdesk for additional information.

Messaging Technologies

Use of email and other messaging technologies shall never be used to transmit confidential or sensitive information in an unencrypted format. Users must pay additional attention to email content and senders and must not open email attachments from unrecognized or suspicious senders. If there are questions about the security of an email, email attachment, or messaging technology users should contact the SSU Information Security Office (security@salemstate.edu). For additional information on the use of email and messaging technologies at SSU, consult the *Electronic Mail (email) Services Policy*.

Information Protection

Users may have access to confidential, sensitive, or public information. Refer to the SSU *Data Classification Policy* to understand what data falls into these categories and how it should be protected. It is not permissible for users to acquire, or attempt to acquire, access to protected data unless such access is granted per the *Access Control Policy*. Under no circumstances may users disseminate any protected information, unless such dissemination is required.

Incident Response

The SSU ITS staff is tasked with responding to all electronic information technology security related incidents, such as computer virus infections. In order to effectively respond to these events, the ITS staff relies on timely information and reporting from users and are guided by the *Incident Response Policy.* Subsequently, users are required to contact the ITS Security Officer (security@salemstate.edu) or other SSU ITS staff if:

- They observe unauthorized or suspicious activity;
- They know or suspect that a security incident has or is going to occur.

Authentication Factors

Most of SSU's information technology resources require the use of a unique user account, password and some form of multifactor authentication. It is important for SSU users to create strong passwords and protect these passwords. To this end, users must never share their passwords or other authentication factors with anyone else, must maintain privacy of their password and these factors, and must promptly notify ITS personnel if they suspect their passwords or authentication factors have been compromised. For additional information on authentication use and protection, refer to the SSU *Authentication Policy*.

Physical and Environmental Security

Assistance from users is required to ensure a physically and environmentally secure working environment. Users are required to be aware of locking and access restriction mechanisms and must proactively challenge unidentified or unescorted personnel within restricted areas of the campus. Users who leave their devices unattended must log off or lock the system before leaving. Refer to the *Physical Security Policy* for more information.

Problem Management

Users are required to report problems or issues discovered with SSU information technology resources to the SSU Helpdesk immediately following discovery. See the *Problem Management Policy* for more details.

Information Security Awareness Training

SSU employees are required to attend security awareness training upon hire and at least annually thereafter. For additional information on SSU's Security Awareness program, refer to the *Security Training and Awareness Policy*.

Role

ITS Management Team: Ensure awareness of this policy. Ensure that this policy and all component policies and procedures are maintained and implemented. Review this policy periodically and update as needed in response to environmental and/or operational changes.

All Users: Understand and adhere to this policy. Use SSU resources in only those methods, which have been identified as acceptable by this policy. Immediately report unauthorized or suspicious activities or violations of this policy to their manager and the ITS Chief Information Security Officer.

Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including loss of access rights and/or termination of employment under adherence to their respective collective bargaining agreement. Students found to have violated this policy may have their access removed and may have additional actions taken as directed by the Student Code of Conduct.

Security Level Public