Security Awareness Training Policy

I. PURPOSE

This policy is intended to set the training standard for several key audiences in Salem State University, including, but not limited to: University executives, business department managers and their staff, the Chief Information Officer and staff, and the faculty, students and related academic community who are serviced or otherwise informed by access to services available on University information systems. This community also includes system and application owners, their contractors and their training coordinators. The success of the University’s awareness and training program, and the overall awareness of secure business practices, depends upon the ability of all users to work toward a common goal of protecting the University’s information and technically related resources.

II. SCOPE

This policy refers to all University information resources whether individually controlled or shared, stand-alone or networked. It applies to all computer and communication facilities owned, leased, operated, or contracted by the University. This includes networking devices, personal digital assistants, telephones, wireless devices, personal computers, workstations, minicomputers and any associated peripherals and software, regardless of whether used for administration, research, teaching or other purposes.

III. POLICY

The policy of Salem State University is to ensure that all individuals are appropriately trained in how to fulfill their operational and access responsibilities before allowing them access to University systems. Such training shall ensure that employees are versed in the rules of the system, and apprise them about available technical assistance and technical security products and techniques. Behavior consistent with the rules of the system and periodic refresher training shall be required for continued access to the system.

Before allowing individuals access to an application, the University will ensure that all individuals receive specialized training focused on their responsibilities and the application rules. This may be in addition to the training required for access to a system. Such training may vary from a notification at the time of access (e.g., for members of the public using an information retrieval application) to formal training (e.g., for an employee that works with a high-risk application, including contractors and other users of information systems that support the operations of the University).

IV. ROLES AND RESPONSIBILITIES

While it is important to understand the policies that require the University to develop and implement a security awareness and training program, it is crucial that University users understand who has responsibility for security awareness and training. This section identifies and describes those within the University who have that responsibility.

Vice Presidents
These executives must ensure that high priority is given to effective security awareness and training for their staff. This includes implementation and support of University initiated programs and the development of additional awareness training programs as they deem appropriate. Department Vice Presidents should:

- Designate a security manager(s) for the departments under their responsibility;
- Assign responsibility for the administration of security awareness training;
- Ensure that a department-wide security awareness program is implemented, is well supported by resources and budget, and is effective; and
- Ensure that each business office has enough sufficiently trained personnel to protect its information resources.

**Chief Information Officer**

The Chief Information Officer is tasked with the responsibility to assist in the development of security awareness training and oversee personnel with significant responsibilities for information security. The Chief Information Officer should work to:

- Establish a University-wide strategy for the security awareness and training program;
- Ensure that the Vice Presidents, business office managers, system and data owners, and others understand the concepts and strategy of the security awareness and training program, and are informed of the progress of the program’s implementation;
- Ensure that the University’s security awareness and training program is funded;
- Ensure the identification and training of an IT department security training administrator;
- Ensure that all users are sufficiently trained in their security responsibilities;
- Ensure that an effective information security awareness effort is developed and employed such that all personnel are routinely or continuously exposed to awareness messages through posters, e-mail messages, logon banners, and other techniques; and
- Ensure that effective tracking and reporting mechanisms are in place.

**Information Technology Security Administrator**

The IT security training administrator has tactical-level responsibility for the awareness and training program. In this role, the program manager should:

- Ensure that awareness and training material developed is appropriate and timely for the intended audiences;
- Ensure that awareness and training material is effectively deployed to reach the intended audience;
• Ensure that users and managers have an effective way to provide feedback on the awareness and training material and its presentation;

• Ensure that awareness and training material is reviewed periodically and updated when necessary; and

• Assist in establishing a tracking and reporting strategy.

**Business Office Managers**

Business office managers have responsibility for complying with the security awareness and training requirements established for their users. These managers should:

• Work with the CIO and the security training administrator to meet shared responsibilities;

• Serve in the role of system owner and/or data owner, where applicable;

• Consider developing individual development plans for users in roles with significant security responsibilities;

• Promote the professional development and certification of the IT security program staff, full-time or part-time security officers, and others with significant security responsibilities;

• Ensure that all users (including contractors) of their systems (i.e., general support systems and major applications) are appropriately trained in how to fulfill their security responsibilities before allowing them access;

• Ensure that users (including contractors) understand specific rules of each system and application they use; and

• Work to reduce errors and omissions by users due to lack of awareness and/or training.

**IT Security Administrators and Business Office Security Managers**

These personnel are in positions that are responsible for the security of the University’s information and information systems. Because of their positions, they can have the greatest positive or negative impact on the confidentiality, integrity, and/or availability of University information and information systems. Specialized role-based information security training is necessary to help ensure that these “keys to security” clearly understand that information security is an integral part of their job; what the organization expects of them; how to implement and maintain information security controls; mitigate risk to information and information systems; monitor the security condition of the security program, system, application, or information for which they are responsible; and/or what to do when security breaches are discovered. These personnel must:

• Attend role-based training identified/approved by their management,

• Advise their management of additional training that can help them better secure information and information systems for which they are responsible, and
• Apply what is learned during training.

Users

Users are the largest audience in any organization and are the single most important group of people who can help to reduce unintentional errors and information system vulnerabilities. Users may include employees, contractors, foreign or domestic guest researchers, other agency personnel, visitors, guests, and other collaborators or associates requiring access. Users must:

• Understand and comply with University security policies and procedures;
• Be appropriately trained in the rules of behavior for the systems and applications to which they have access;
• Work with management to meet training needs;
• Keep software/applications updated with security patches; and
• Be aware of actions they can take to better protect the University’s information. These actions include, but are not limited to: proper password usage, data backup, proper antivirus protection, reporting any suspected incidents or violations of security policy, and following rules established to avoid social engineering attacks and rules to deter the spread of spam or viruses and worms.

V. REPORTING SECURITY INCIDENTS

Reporting incidents is an ethical responsibility of all members of the Salem State University community. A critical component of security is to address security breaches promptly and with the appropriate level of action. The IT Incident Management Policy outlines the responsibilities of departments and individuals in reporting as well as defining procedures for handling security incidents. No one should take it upon themselves to investigate the matter further without the authorization of the University’s Chief Information Officer or General Counsel.

VI. VIOLATION OF POLICY

Violation of this policy may subject a user to disciplinary action under appropriate University disciplinary procedures. The University may take such action as necessary, in its discretion, to address any violation(s) under this policy.

VII. SUPPLEMENTAL REGULATIONS AND STANDARDS

Acceptable Use Policy: Salem State University standard for acceptable use of University online services.

Incident Management Policy: Salem State University standard for the management of incidents involving online services or University data sources used by the University community.

Enterprise Information Security Standards: Massachusetts Data Classification Standard, Version 1.0

Executive Order 504: Massachusetts Executive Order regarding the security and confidentiality of personal information

Public Records Division: Massachusetts Public records resources as provided by the Secretary of the Commonwealth

Identity Theft Law: Massachusetts law relative to security freezes and notification of data breaches (Chapter 82 of the Acts of 2007).


The Family Educational Rights and Privacy Act (FERPA): (20 U.S.C. § 1232g; 34 CFR Part 99) is a Federal law that protects the privacy of student education records.

Electronic Communication Policy: Salem State University standard for the use of University electronic communications.

Gramm-Leach-Bliley Act (GLBA): The Gramm-Leach-Bliley Act applies to "financial institutions," which include not only banks, securities firms, and insurance companies, but also companies providing many other types of financial products and services to consumers.