University Administrative Policies
Policy Name: **Information Security Policy**
Web Link: www.salemstate.edu/policies

| | | |
|---|---|---|
| **Responsible Office:** Information Security<br>**Responsible Official:** Chief Information Security Officer | **Originator of the Policy:** Chief Information Security Officer<br>**Origination Date:** 10/7/2009 | **Effective Date:** 11/9/2015<br>**Revision History**: 1/18/2011, 12/4/2015; 9/20/16 |

## 1. RATIONALE

The purpose of this policy is to provide general guidance on the protection of Salem State's information resources from accidental or intentional access or damage while also preserving and nurturing the open, information-sharing requirements of its academic culture. Information security is critical to the interests of the University and the many constituencies it serves. The purpose of this policy is to:

- Support and maintain the ongoing functions of the University. As an increasing percentage of the University's functions are handled electronically, it is critical that information and information systems be protected so the University can operate without interruption.
- Protect University assets. The University is in possession of many assets including intellectual property, research and instructional data systems, and physical assets. Loss of these assets could have significant financial impact as well as major negative impact on critical research and instructional programs.
- Safeguard the privacy of individuals and information. With the increasing risk of identity fraud and other potential misuses of personal information, it is paramount that the University safeguards personal information entrusted to its stewardship.
- Safeguard financial transactions and electronic communications. The University is the custodian of financial records and transactions; safeguarding these records is critical to maintaining trust relationships essential to our business functions.
- Protect the integrity and reputation of the institution. Security breaches reflect negatively on the capability of the University to manage entrusted resources. In addition, security breaches could result in the potential for criminal or civil action.
- Prevent the use of University systems for malicious acts. The open nature of the University and the desire to provide ease of access to a large and diverse group of constituents makes us a target for unauthorized users to utilize University resources inappropriately. The

University must prevent the use of Salem State University systems and infrastructure for malicious acts against its own systems as well as attacks against other individuals and organizations.

- Comply with state and federal laws. State and federal laws and regulations require the University to take reasonable steps to ensure the security of the data (FERPA, HIPPA, and GLBA). Failure to safeguard this information could result in the legal action or cause the University to lose its ability to offer services.

## 2. STATEMENT OF POLICY

Information that Salem State University personnel or its agents use in the course of conducting University business is an institutional resource. Every member of the University community is responsible for the security and protection of information resources over which they have control. Although individuals, offices, departments, programs or schools may have responsibilities for creating and maintaining portions of this information or records, the University itself retains ownership of, and responsibility for, that information.

Access to these data is to be granted only to those University employees who must use these data to pursue University business. With special permission, a student may access data if the data pertains to that student or if that student is also an employee of the University. Individuals outside the University can be authorized access to University data only if that authorization is granted by an Executive Officer of the University.

## 3. SCOPE

This policy is applicable to all University students, faculty and staff and to all others granted use of Salem State University information resources. Every user of the University's information resources has responsibility toward the protection of those assets; some offices and individuals have very specific responsibilities. 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.

## 4. ROLES AND RESPONSIBILITIES

### Chief Information Security Officer:

Has overall responsibility for the security of the University's information technology assets and is responsible for disseminating and providing interpretation of this and other related policies related to security. Responsibilities of this Office include:

- Ensuring that appropriate data security policies are delegated throughout the University to various University services, departments and other units; and to individual users of campus technology resources.

- Creating Security Champions. The Security Champions are responsible for the development of policies and procedures to ensure the security, integrity and accuracy of the University's data including student and employee data, financial data and other official institutional data. Members of the Committee will include mid-level functional managers from University departments responsible for the creation, retention, and use of these data;
- Serving as the chair of the Security Champions;
- Ensuring adequate security technology is applied to information resources in keeping with their classification;
- Ensuring that all data security policies within the University are complied with on an acceptable basis;
- Ensuring the monitoring of University data sources for indicators of data loss, loss of data integrity, intrusion or breach of data security;
- Being the initial point of contact for all security incident follow-up procedures and the coordination of these procedures with University executives, the University general counsel, and law enforcement;
- Promptly reporting to the General Counsel and Vice President of Administration any security incidents arising from a breach in established data security policies; and Annually reviewing, in conjunction with the Data Custodians, that all access capabilities granted to all individuals on the system is current and accurate and that no changes are necessary.

**University Vice Presidents:**

Will ensure that appropriate information security procedures are developed, published, distributed and implemented within their areas of responsibility. In addition, they are responsible for:

- Designating and managing the efforts of one or more data custodians for all information resources maintained in their area of responsibility;
- Ensuring that all staff in their areas have the training and support necessary to protect data in accordance with this policy; and
- Approving access authorization of all information uses in their area of responsibility having a data classification of Confidential;

**Data Custodians:**

Are responsible for making decisions about the use and protection of information in their custody. These responsibilities include:

- The accuracy and completeness of data and information; − the classification of data as confidential (subject to privacy laws), sensitive (non-public salary information) or public;
- An authorization approval process permitting access to the information and the termination of that access when necessary; − the identification and minimization of risks and exposures;
- The utilization of established procedures designed to protect information from unauthorized access or disclosure, whether accidental or intentional;

- Ensuring that issues impacting the quality of data within their responsibility are properly reported and adequately resolved in a timely manner;
- The proper communication of information protection procedures to authorized users;
- The physical access to hard copy records, computer terminals and personal computers;
- The provision of procedural safeguards including backing up information for business continuity purposes;
- Supporting the Chief Information Officer in the follow-up actions required to take appropriate actions in the resolution of all security incidents;
- The evaluation of security control procedures related to University information in their custody; and
- The annual review, in conjunction with the Chief Information Officer that all access capabilities granted to all individuals on the system is current and accurate and that no changes are necessary.

**Individual Users:**

Include all persons who have been authorized to access or update University information sources. They have the responsibility to:

- Become familiar with and comply with all University, State and Federal security regulations and policies related to data protection, technology use and privacy rights;
- Use the information only for the purpose that was authorized by the custodian for that information;
- Ensure that their personal access information is not lost, stolen or shared with any unauthorized users;
- Ensure that all remote access from University or home computers meet the security guidelines established for campus users;
- Comply with all controls established by the custodian and those delegated by the custodian to administer control procedures; and
- Avoid disclosure of confidential or sensitive information to unauthorized persons without the permission of the custodian.

**Individuals as Owners of Computers and Other Network Devices:**

- Are responsible for the security of their personally-owned computers or other network devices and therefore must ensure that their personal equipment meets all security policies, standards and guidelines for best practices for users of University computing and network facilities.

## 5. 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 will outline 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.

## 6. POLICY ENFORCEMENT

| | |
|---|---|
| Violation(s) | It shall be a violation of this policy for data to be received, sent or stored inconsistent herewith. |
| Potential consequences | Appropriate discipline. |
| How to report | Contact Chief Information Security Officer |

## REFERENCE DOCUMENTS

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

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

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 Fair Information Practices Act: Massachusetts fair information practice standard (Mass. Gen. L. ch. 66A).

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.

Freedom of Information Act: Federal Freedom of Information Act (FOIA).

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.

HIPAA Security Regulations: Federal compliance guidelines for the Health Insurance Portability and Accountability Act of 1996

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

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

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

Website Privacy Policies: Massachusetts requirements for agency website privacy.

## 7. CONTACT(S)

| Subject | Office or Position | Telephone Number | Email |
|---|---|---|---|
| Policy Clarification | CISO | 978-542-2745 | tcesso@salemstate.edu |

## 8. APPROVALS/ENDORSEMENT/NOTICE REQUIRED

| Level | Title & Name | Signature | Date |
|---|---|---|---|
| Chair or Director of Department or Office | CISO/Thomas Cesso | | |
| Dean or Assistant Vice President | Gene Labonte | | |
| Vice President | John Keenan | | |
| P.E.C. Initial Review | | | |
| P.E.C. Final Review | | | |
| All University Committee | | | |
| President | Patricia Maguire Meservey | | |
| Board of Trustees (notice) | | | |

## 9. REVIEW CYCLE

Initial review after 12 months