University Administrative Policies
Policy Name: Security Training and Awareness Policy

Responsible Office: HR and Information Security **Responsible Officials:** VP of HR, CISO, CIO	**Originator of the Policy:** Patricia Ainsworth **Origination Date:** 3/25/16	**Effective Date:** 3/25/2016 **Revision History:** 11/28/2016

PURPOSE

The purpose of this policy is to ensure that any employee who has access to Salem State University's (SSU) information technology resources has an understanding of the applicable information security policies at Salem State and access to training.

SCOPE

This policy applies to all employees and contractors who have access to Salem State's information technology-based resources containing Confidential Data per the SSU Data Classification Policy.

POLICY

The primary purpose of an effective information security awareness training program is to establish and sustain an appropriate level of protection for data and information resources by increasing users' awareness of their information security responsibilities. Specific objectives include:

- Improving awareness of the need to protect information resources;
- Maintaining compliance with MA 201-CMR 17, PCI-DSS; HIPAA
- Ensuring that users are knowledgeable about the university's information security policies and practices, and develop skills and knowledge so they can perform their jobs securely.

All users who have access to Confidential Data will be required to complete Security Awareness training upon hire and subsequently at least annually. Salem State will maintain records, as it deems appropriate, that confirm that a user has received training. Training may be delivered in person or online.

The Human Resources Talent Development Coordinator is responsible for managing the IT Security Training and Awareness program and will inform users of their requirements, monitor compliance with the training requirement, and update management regarding the compliance of their employees.

The Manager approving a Statement of Work for contractors who will have access to Confidential Data is responsible for ensuring the contractor takes the security and awareness program as part of engagement negotiation process.

ENFORCEMENT

Any person found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action, up to and including loss of access rights, termination of employment.

ROLES AND RESPONSIBILITIES

ROLE	RESPONSIBILITY
CISO	Ensures development and approves content of the Information Security Training and Awareness program.
Human Resources	Facilitates the Information Security Training and Awareness program, ensures all personnel receive the appropriate security training associated with their jobs, and maintain records of training received.
Managers	Ensures contractors who will have access to Confidential data have taken the Information Security Training and Awareness program prior to engagement and system access.
Data Custodians and Management	Ensure that all employees who will have access to confidential data are appropriately trained and understand their roles in implementing the university's Information Security Policies.
All Users with access to Confidential data	Complete annual security training. Review, understand and agree to comply with all university information security policies and guidelines.

REVISION HISTORY

This section contains comments on any revisions that were made to this document and the date they were made.

Version Number	Issued Date	Approval	Description of Changes
1.0	3/25/16	Patricia Ainsworth, CIO/CISO John Keenan, General Counsel and VP of Administration Patricia Maguire Meservey, President	Initial Draft

Version Number	Issued Date	Approval	Description of Changes
		Notification of All University Committee	
2.0	11/28/2016	Thomas Cesso, CISO Mark Quigley, AVP, Human Resources John Keenan, General Counsel/VP for Administration Patricia Maguire Meservey, President Notification of All University Committee	First Issue