Salem STATE | UNIVERSITY

University Administrative Policy

Policy Name: Encryption Policy
Responsible Office: CISO, CIO
Originator of the Policy: CISO, CIO
Effective Date: July 11, 2016
Revision History:
Web Link: https://www.salemstate.edu/policies/

---

1. Rationale

The purpose of this policy is to provide the information security requirements at Salem State University (SSU) for the use of encryption algorithms to protect confidential information.

2. Statement of Policy

Salem State University shall use approved encryption to protect confidential information. Salem State University must use only approved cryptographic techniques and follow Federal regulations and adhere to legal authority that is granted for the dissemination and use of encryption technologies outside of the United States.

3. Scope

This policy applies to the encryption used to protect confidential information. A risk-based approach drives all SSU data encryption requirements. Considerations include legal or regulatory requirements, data inventory, classification, method(s) of access, storage or transmission mechanisms, and other contributing security controls in place.

This policy applies to confidential data as defined in the SSU Data Classification policy whether in transit across a public network or at rest on laptops and portable devices. Encryption of all transmitted records and files containing personal information that will travel across public networks, and encryption of all data containing personal information to be transmitted wirelessly, is within scope.

4. Fiscal Considerations

	Direct Costs / Savings / Revenue Generation	**Indirect Costs / Savings / Revenue Generation**
Initial Implementation	Varies over time	Varies over time
Ongoing	Varies over time	Varies over time

5. Responsibilities

Responsible Party	List of Responsibilities
CISO	Ensure awareness and compliance with this policy.
CIO	Ensure that this policy and all component policies and procedures are maintained and implemented
Managers/Supervisors	Ensure Confidential data are encrypted per this policy.
All Users	Understand and adhere to this policy.

6. Policy Enforcement

Violation(s)	It shall be a violation of this policy to promulgate any applicable policy in contravention of the requirements outlined herein.
Potential consequences	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 or expulsion from the University
How to report	Contact CISO or CIO

7. Reference Documents

Policy or Document	Web Address
PCI/DSS	
MA 201 CMR 17.00	
HIPAA	

8. Contact(s)

Subject	Office or Position	Telephone Number	Email
	CIO, CISO		

9. **Effective Date:** Upon approval by the president.

10. **Dissemination:** Posted on the university web site.

11. **Review Cycle:** Initial review after 12 months; subsequent review every 5 years.