University Administrative Policy

Policy Name: **Configuration Management**
Responsible Office: Information Technology Services
Originator of the Policy: Chief Information Officer
Effective Date: October 31, 2016
Revision History:
Web Link: https://www.salemstate.edu/policies/

---

1. Rationale

The purpose of this policy is to define the mechanisms for creating and maintaining a secure information technology environment for Salem State University (SSU) information resources.

2. Statement of Policy

All SSU systems shall be configured and managed using secure and industry vetted best practices. SSU system configuration standards shall be designed in accordance with industry best practices. Management of SSU systems includes the following activities:

- Event and system log monitoring.
- Malware prevention and response.
- Installation of system updates and patches.
- Device maintenance and repair.
- Changing default system and application passwords.

3. Scope

This policy applies to all SSU systems, specifically servers, network devices, and workstations.

4. Fiscal Considerations

	Direct Costs / Savings / Revenue Generation	**Indirect Costs / Savings / Revenue Generation**
Initial Implementation		
Ongoing		

5. **Responsibilities**

Responsible Party	List of Responsibilities
CIO	Ensure awareness and compliance with 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. Review and approve all system configuration standards and associated procedures.
IT Managers IT Staff	Implement system configurations in accordance with SSU configuration standards and procedures. Review and respond to system and event log alerts. Distribute and manage malware prevention mechanisms. Respond to and remove malware infections. Distribute and manage system updates and patches.

6. **Policy Enforcement**

Potential consequences	Any employee found to have violated this policy, intentionally or unintentionally, may be subject to disciplinary action up to and including termination of employment.
How to report	Contact CIO

7. **Reference Documents**

Policy or Document	Web Address
PCI MA 201 CMR 17.00 HIPAA	

8. **Contact(s)**

Subject	Office or Position	Telephone Number	Email

9. **Effective Date:** Upon approval.

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

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