University Administrative Policy

Policy Name: **Change 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 control all changes to Salem State University (SSU) production systems. Changes require serious forethought, careful monitoring, and follow-up evaluation. to reduce negative impact to the community and to increase the value of Information Resources.

2. Statement of Policy

All production system changes shall be planned, approved, tested and documented.

- Only authorized staff shall perform changes.
- Assessment of the potential impact of such changes shall be conducted.
- Audit trail of all changes, configuration changes made, person who performed the change, date of the change, purpose of the change, and other relevant information shall be retained.
- Procedures for testing and approval of changes shall be implemented prior to promotion to production.
- Procedures identifying responsibilities for aborting and recovering from unsuccessful changes shall be implemented.
- Information users shall be notified regarding how these changes shall impact them. If system availability will be affected while the change is being made, affected individuals will be notified letting them know what to expect and when to expect it. They should also know whom to contact in case they experience difficulty as a result of the change.
- Current backups shall be available when changes are made.
- The Production/Change management team shall review changes prior to installation into a production environment to ensure all relevant procedures were followed except in emergency situations.
- A change may be denied for reasons including, but not limited to, inadequate planning, inadequate back out plans, the timing of the change will negatively impact a key business process such as year-end accounting, or if adequate resources cannot be readily available.

- System failures or the discovery of a critical vulnerability affecting security may necessitate emergency changes.
- All changes shall be reviewed to ensure that organizational documentation (user documentation, network diagrams, procedures, knowledge bases, etc.) impacted by the change is updated accordingly.

3. Scope

This policy applies to all changes to SSU production systems including applications, hardware, and systems.

4. Fiscal Considerations

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

5. Responsibilities

Responsible Party	**List of Responsibilities**
CIO **IT Directors**	Ensures change control policies and procedures are followed according with this policy.
IT Staff	Follows this policy and shall maintain a log with the change documentation. Ensure that changes to systems have been approved, documented, tested and implemented in compliance with the policy.

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.