University Administrative Policy

Policy Name: **Information Technology Access Control Policy**
Responsible Office: Information Technology Services
Originator of the Policy: Chief Information Officer
Effective Date: March 25, 2016
Revision History: October 31, 2016
Web Link: https://www.salemstate.edu/policies/

---

1. Rationale

The purpose of this policy is to control and manage access to Salem State University's (Salem State) information technology-based resources.

2. Statement of Policy

All access to Salem State applications, systems and hardware shall be authorized and approved by the employee's supervisor. Any access not explicitly authorized and approved is prohibited. Access to specific applications, systems, components and technology infrastructure shall only be granted to personnel with a legitimate business need as approved by their supervisor. The level of access granted and privileges assigned shall be limited to the minimum required in order to do their jobs effectively.

3. Scope

This policy applies to any user who accesses Salem State's information technology-based resources.

4. Fiscal Considerations

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

5. Responsibilities

Responsible Party	**List of Responsibilities**
CISO	Ensure awareness of and compliance with this policy.
CIO	Ensure that this policy and all component policies and procedures

	are maintained and implemented.
IT Staff (Application Security)	Design, setup, monitor, test application security. Document access control procedures. Implement approved access to specific applications, systems, components and technology infrastructure to personnel with a legitimate need. The level of access granted and privileges assigned shall be limited to the minimum required to perform assigned duties. Distribute access control lists for quarterly reviews.
Human Resources Staff	Notify IT of new employees, terminated employees and changes in job responsibilities that would affect access rights.
Managers/Supervisors	Determine who should have access to information technology resources. Periodically review access rights and notify IT when access privileges require adjustment per the SSU Data Classification Policy.
All Users	Understand and adhere to this policy. Safeguard their user IDs and passwords. Access only those resources for which they are authorized. Immediately report suspected violations of this policy to their manager or the IT Manager.

6. Policy Enforcement

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.
How to report	Contact CIO

7. Reference Documents

Policy or Document	**Web Address**	
Framework Critical Security Controls	Regulations and Requirements PCI DSS - MA 201 - HIPAA	Supporting Standards and Procedures Data Classification Policy Acceptable Use Policy Other current information technology policies

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.