University Administrative Policy

Policy Name: **Administrative Rights**
Responsible Office: Information Technology Services
Originator of the Policy: Chief Information Officer
Effective Date: May 2, 2016
Revision History: October 31, 2016
Web Link: https://www.salemstate.edu/policies/

---

1. Rationale

Computers are provided to University faculty and staff, which are given User permissions to their desktop or laptop. A higher set of permissions is called "administrative rights".

The granting of administrative rights to an employee of Salem Statue University (SSU) over an individual desktop, laptop, or other end-user device is a privilege only awarded to individuals who require this level of access and control in order to do their jobs effectively. The goal of this policy is to describe the circumstances under which administrative rights can be granted as well as the terms and conditions upon which this privilege will be granted.

2. Statement of Policy

The granting of administrative rights allows the end user to make administrative changes to their computer. As a result, these rights can expose the SSU network to malware and other security exploits. In addition, incorrect configuration of machines can lead to performance problems, potentially resulting in machine downtime, lost productivity, higher support costs, and data exposure.

Given the serious consequences of mishandling or abuse of administrative rights, these rights will only be granted under the condition that they are essential for the performance of the grantee's job. Such conditions could include the following:

The ability to download and install specific types of software or configure system settings is mandated in the individual's job description. This includes faculty who need to evaluate student work that may be in the forma or software.

Typically, the only individuals at SSU who are granted administrative rights include:

Job Title	Requirement for Administrative Rights
Desktop Support Technician	Set up desktops and laptops for end users. Provide desk-side and remote support to desktop and laptop users.
Department Technical Support	Manage & support desktops within their department as part of their job description. Ex: library, lab managers.
Faculty	Who request the right based on academic freedom reason. If a faulty member causes a security incident, they will lose this privilege.

Note: Members of the IT department are not automatically granted administrative rights based on their membership in the IT department alone.

The determination of whether Administrative Rights are necessary for employees to effectively perform their job duties will be decided collaboratively between the Information Security team and business unit managers. Any changes should be tested on a few systems in the business unit before being rolled out to the rest of the systems to minimize possible disruption to business processes.

Roles and Responsibilities:

If you have been granted administrative rights, you must adhere to the following roles and responsibilities:

a. You will comply with all existing and future technology policies of SSU.

b. You will not grant admin rights to others on your machine based on your privileges.

c. You will not install any unauthorized or non-standard unlicensed software at any time.

d. You will take all reasonable steps to ensure that the desktop, laptop or other end-user device over which you have administrative rights is secured from malware or intrusion.

e. The ITS department will provide support and troubleshooting for the standard base image issued with the machine.

f. Your administrative rights can be terminated at any time if the terms of this or any other technology policy are violated.

g. You should never log in to any computer directly with administrative rights. Rather, you should temporarily elevate your rights when needed.

3. Scope

This policy applies to employees and contractors who handle Confidential information as defined in the SSU Data Classification policy. Employees and contractors who handle only Sensitive or Public information per the Data Classification policy are not within the scope of this policy since these data are not protected by security/privacy laws.

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 and compliance with this policy.
CIO	Ensure that this policy and all component policies and procedures are maintained and implemented.
IT Staff (Helpdesk)	Implement approved administrative access on specific systems to personnel with a legitimate need.
Human Resources Staff	Notify IT of new employees, terminated employees and changes in job responsibilities that would affect administrative access rights.
Managers/Supervisors	Determine who should have administrative rights in order to perform job duties in collaboration with Information Security. Periodically review administrative access rights and notify IT when access privileges require adjustment.
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 or expulsion from the University.
How to report	Contact CIO

7. **Reference Documents**

Policy or Document	Web Address

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.