Workstation Elevated Permissions Authorization and Procedures

Office: Information Technology

Procedure Contact: Chief Information Officer

Revision History

Revision Number:	**Change:**	**Date:**
2.0	Updates and conversion to new format.	**08/29/2013**
2.1	Format changes	**03/24/2014**
2.2	Removal of OUS references	**09/16/2016**

A. Purpose

This procedure establishes guidelines for granting elevated workstation permissions to faculty, staff, and student employees and the responsibilities inherited by these employees when granted these rights. These guidelines exist to ensure SOU confidential information and technologies are not compromised, that production services and other SOU interests are protected from user activities, and that there is an understanding about support availability.

B. Definitions

Administrative User - The least restrictive user security model. The user is able to install any software and make configuration changes. The workstation has very little protection from unintended changes or software installations including viruses and malware.

Elevated Permissions - Users granted administrative permissions on a workstation have unrestricted access to the operating system and data storage. They can create, delete and modify any of the files or folders on the computer, as well as, change any settings. This level of access is typically reserved for IT staff members.

Standard User - The most restrictive (secure) user security model. Users can install software written to work properly with the standard user security model.

Workstation – a university-owned laptop or desktop.

C. Procedure

1. User Account Permissions

Information Technology industry best practices suggest, and Southern Oregon University's Internal Audit Division has required, that SOU user accounts be granted the minimum permissions required to perform their work-related activities.

By default, all SOU user accounts are provisioned with standard user permissions. While this is an effective means of increasing the security and reliability of computing resources, it can prevent some legitimate uses. For example, some software packages do not operate properly with standard user permissions. While alternate solutions are often possible, granting elevated permissions is sometimes required.

2. Responsibilities of Having Elevated Permissions

Appropriate measures must be taken by employees when using workstation(s) with elevated permissions to ensure the confidentiality and integrity of sensitive information, including protected SOU information, and to minimize the possibility of unauthorized access. Additionally, the employee is responsible for any and all information stored on their workstation, such as software, account information, stored passwords, and web browser data.

Employee responsibilities include, but are not limited to:

- Complying with the SOU Computing Resources Acceptable Use Policy.
- Restricting physical access to workstations to only authorized personnel.
- Securing workstations (screen lock or log-out) prior to leaving area to prevent unauthorized access.
- Enabling a password-protected screensaver with a short timeout period to ensure that workstations that were left unsecured will be protected.
- Complying with all applicable password policies and procedures.
- Ensuring workstations are used for authorized business purposes only.
- Never installing unfamiliar or suspicious software on workstations.
- Storing all sensitive information on secure, SOU-provided network servers.
- Securing laptops containing sensitive information by using cable locks or in lockable drawers or cabinets.
- Ensuring workstations are still capable of receiving SOU-provided updates, upgrades, and installations.
- Understanding that support may be limited in some cases of extreme workstation divergence from standard configurations.

Any employee found to have violated these guidelines may have their elevated permissions revoked.

3. Common Reason for Granting Elevated Permissions

The following is a list of common scenarios when elevated permissions are granted:

Applications Requiring Administrative Rights: In some circumstances, it may not be possible to make an application run properly with standard user permissions. If the application will be used by an individual, they will be made an administrative user on their workstation. If the application will be used in a class, the members of the CRN will be made administrative users on the workstations in the lab where the class is taught.

Frequent Software Installation/Maintenance: Employees who have a frequent need to install software on their workstation may be granted administrative permissions for their workstation.

Extended Travel: Employees traveling overseas or who will be away from campus for an extended period (typically over 90 days), may be granted elevated permissions since IT support will not be readily available.

4. Requests for Elevated Permissions

All requests for elevated permissions should be made through the appropriate Information Technology department Computing Coordinator or the IT Help Desk. The Chief Information Officer or User Support Manager must approve all requests.

This procedure may be revised at any time without notice. All revisions supersede prior procedures and are effective immediately.

C. Associated Procedures or Other Information

SOU Information Security Policy FAD.040
SOU Acceptable Use Policy FAD.038