

Seattle University Computer Administrative Permissions Policy

I. Overview

Computer users typically have two types of permissions on computers owned by Seattle University. General permissions, which allow the faculty or staff person to complete daily tasks, use programs, access email, browse the web and customize most settings to suit their needs. General permissions require help from OIT to add or remove programs and set advanced configuration and network options. Administrative permissions give users complete access to their computer and the underlying operating system. Users can add/remove programs, change permissions for all users and make changes to the operating system.

To safeguard the security and data integrity of university computing resources and networks, Seattle University requires that all faculty and staff who would like administrative permissions on a university-owned computer obtain the permission of their supervisor, articulate the need for permissions and register with The Office of Information Technology (OIT). This helps the university and OIT provide a secure and stable computing environment for students, faculty and staff. More specifically, closely monitoring administrative permissions has the following benefits:

- Helps with proper management of SU licensed software.
- Prevents installation of unlicensed software on SU owned hardware.
- Prevents potentially unsafe third-party software containing spyware or other malicious software from being installed.
- Frees up technical support resources by creating a standard computer configuration.
- Enhances network security and stability by ensuring that anti-virus technology cannot be uninstalled or disabled.

In most cases, general permissions meet the needs of faculty and administrative staff with OIT providing support when needed. However, especially in academic environments, there are a number of reasons a user might need temporary or permanent administrative permissions. Examples might include cases where licensed software will not run on the machine without elevated permissions, the user provides technical support for their department or school, or where the user teaches or works in a technology field requiring frequent access to advanced administration options.

II. Scope

This policy applies to all users and computers owned by the university, connected to university networks and supported by the Office of Information Technology. This policy is effective August 1, 2007.

III. Policy

By default all faculty, staff and students working on computers and similar devices owned by the university, connected to university networks and/or supported by OIT will be granted general user permissions to their computer. Users who require administrative permissions in the course of their academic or administrative work are required to

- obtain the written approval of their immediate supervisor,
- document the need for elevated permissions,
- complete official SU FERPA training or provide proof of recent training,
- read and sign all documentation.

Approval of administrative permissions is the responsibility of the supervisor of the requestor, as defined by the department, division, college or school where they are employed. OIT will administer and keep records associated with the program, but will not directly approve or deny permission requests.

Final draft – 08/22/07 - Joe Eastham, Web Communications

Seattle University Computer Administrative Permissions Policy

The university recognizes that faculty and those that support them sometimes have computing needs beyond that of an average business user. Seattle University is committed to providing access to technology, including administrative permissions, to those engaged in academic work and the educational mission of the university.

IV. Process

1. The requestor fills out the form provided in its entirety, taking care to read and assent to the responsibilities and risks that come with elevated permissions and completes FERPA training if necessary.
2. The user then obtains written permission from their supervisor and either the supervisor or user submits the paperwork to OIT via the Help Desk.
3. OIT processes the request, contacts the user (and supervisor if necessary) and determines if the permissions need is temporary or permanent.
4. A ticket is opened and desktop support staff dispatched to grant the agreed upon permissions.

For help with permissions issues and questions about the process, please contact the OIT Help Desk at 206-296-5571 or via email at helpdesk@seattleu.edu. Comments about this policy should be directed to the Office of the University Counsel at 206-296-2043.