Fairfield University Computer User Policy

Fairfield University Computer User Policy

It has always been the policy of the IT department at Fairfield University to ensure the security of information owned by the students and their families as well as that of our faculty and staff. A constantly changing IT environment introduces new challenges at an ever increasing pace and while information security has always been a priority the challenges of managing our infrastructure have increased exponentially. University policy has always been to minimize potential information leakage risk to everyone on campus. This is a difficult task at best but one that needs to be addressed and starts at the most basic level; the entrance to our network, that portal to all the information on campus which we all use on a daily basis; university owned devices and computers. In order to access to these devices and computers one must have “Privileges”, not rights, and these Privileges grant the user the ability to perform their daily tasks. Faculty and staff may have a legitimate need for administrative privilege on their computers. Administrative privileges may be required to install software and updates, perform computer management tasks, or run some software packages.

However, using administrative access for everyday tasks such as reading e-mail or browsing the web carries an increased risk. Malicious software can take advantage of administrative privileges to jeopardize the operational integrity of a computer system. Violated accounts with administrative privileges may allow intruders to disrupt computer or network operations, steal information, or allow unauthorized access to data residing on the system or attached devices. Improperly applied administrative privileges may directly impact the availability of both computing resources and IT professional support. For this reason it is prudent to restrict administrative access to those who truly need it for academic or business needs and to refrain from using administrative access for the most risky tasks.

Administrative privileges should only be granted to people with a distinct need. Administrative privileges are granted to anyone with the title Vice President and above. All other Staff can be granted administrative privileges on a temporary basis after demonstrating a specific need. Requests will be made to the help desk, reviewed, denied or granted, and the computer will be remoted into, and the requesting user will have administrative privileges for 24 hours to perform the necessary task. At which time the user’s privileges will be returned to their normal working level.

Levels of Access

There are two security access levels to a University owned computer: User and Administrator.

• User - Allows a great deal of powers to perform normal daily functions. The user access level will generally assure the highest level of stability for your computer.

• Administrator - Allows the client to have complete and unrestricted access level rights on their individual workstations. This includes the ability to install any hardware or software, edit the registry, manage the default access accounts, and change file level permissions.

If you have administrative privileges on a University computer, your responsibilities include:

•Awareness that the administrative account increases the potential for computer or network compromises.

•Install software only from trusted sources (if in doubt, get a second opinion from Technology Support staff).

•Update the software you install. Configure the software you install to automatically apply updates or periodically manually check for software updates.

•Keep the licensing current on all software you install.

•Maintain any service that was included in the initial configuration of your device (such as automated operating system updatespatches, application software patches and anti-virus updates).

•Avoid the following administrative activities: create additional user accounts, change or disable logging settings,

change file permissions or ownership.

The University reserves the right to revoke administrative privileges granted to any user on a University owned system.

All University owned computers must:

•Be joined to the University's Active Directory domain;

•Have management software installed that facilitates hardware or software inventory for asset tracking, license compliance, software installation/upgrading, remote assistance, or troubleshooting;

•Have active, properly configured security (anti-virus, malware, etc.) software;

•Have service packs and/or patches deemed necessary by ITS.

NOTE: Exceptions to the above can be made by the ITS Director.

•User agrees that, in the event their local administrative privileges result in a security compromise, they may be held responsible for any damages that may result to the full extent allowed by University policy, Local, State, and/or Federal law.

Privileges Revocation

A user's local administrative privileges may be revoked for any of the following reasons:

•User is involved in a data breach that is related directly to their having administrative privileges;

•User is downloading or installing software that is illegal or malicious to the University's Information Technology Resources;

•User is downloading or distributing copyrighted material without permission and can't demonstrate "fair use" (http://www.copyright.gov/fls/fl102.html);

•User requires excessive support from ITS staff. Excessive support is defined as frequent incidents requiring ITS staff to spend time returning a computer's operating system or software to a properly functioning state.

The University reserves the right to revoke administrative privileges granted to any user on a University owned system.

Requesting Temporary Computer Administrator Privileges can be accomplished by contacting ITS at extension 2069.

Following industry best practices, ITS does not authorize administrative privileges for Fairfield University user accounts on university computers connected to the Fairfield University domain other than those specified above. ITS grants the least privilege required to perform daily computing tasks. The purpose of this policy is to ensure the uninterrupted operation of university computers, the integrity and security of university information systems, the prevention of unauthorized access to resources, and minimal support costs. This policy is in effect for all ITS supported computers. Non-standard models and personal devices have separate requirements, restrictions, and support structures.

Data Security - university computer users who are granted administrative privileges should be aware that using an account with administrative privileges makes the user computing environment extremely susceptible to spyware, viruses and potentially damaging security breaches. The institution is bound by federal and state law to protect our sensitive data from unauthorized use (FERPA, HIPAA, GLBA).

Data Loss - university computer users who are granted administrative privileges should be aware that they would become fully and solely responsible for any data that is stored locally on the computer they are administering and as such must exercise due diligence in providing a backup mechanism to ensure against the potential loss of any data. Failure to implement a backup mechanism can result in permanent loss of any and all data. ITS is not responsible for data loss, all users are responsible for their own data backup.

Software Licensing & Copyright Laws - university computer users who are granted administrative privileges should be aware of copyright restrictions and licenses placed on ALL software installed on their systems as well

as being aware that there exists severe criminal and civil penalties for noncompliance. University computer users do not have the authorization to agree to any software terms and conditions (End User License Agreements) on behalf of the university. Agreeing to End User License Agreements while installing software on university owned computers may subject the institution to laws of foreign countries and or states other than Connecticut.

For further assistance, please visit the ITS Help Desk located in NYS 230 or call 203-254-4069 during business hours.

Hours can be found here: ITS Help Desk Hours of Operation