California University of Pennsylvania

MANAGEMENT DIRECTIVE: FACULTY ADMINISTRATIVE RIGHTS

Related Policies: ***Acceptable Use Policy (AUP), Information Security Policy, Security Incident Reporting and Response Policy, Data Classification Policy, Password Policy, and Remote Access Guidelines***

A. Purpose & Scope:

The purpose of this directive is to establish guidelines for using administrative computer accounts and the procedure for requesting administrative rights to a computer, or group of computers.

B. Definition(s):

C. Procedure(s):

1. Administrative Accounts

Administrative accounts have an elevated set of privileges that allow users to make changes to system settings, software and hardware. They also come with increased risks of viruses, malware, and system problems.

As a security best practice, those requesting administrative rights will have a second Active Directory user account created that will include –admin after the user name (i.e. Smith-admin). The user requesting the account will agree to the following restrictions:

- Administrative accounts will only be used to perform tasks requiring administrative privileges;
- Administrative accounts will not be used for general day-to-day activities such as logging into your computer or e-mail and web access;
- Administrative accounts will not be used to remove or modify any hardware without UTech's permission;
- Administrative accounts will not be used to disable or reconfigure the remote management services used by UTech;

- Administrative accounts will not be used to disable or reconfigure security controls (ex. antivirus, firewall, automatic download of patches, audit log settings);

- Administrative accounts will not be used to create additional user accounts, give any other accounts administrative access or otherwise tamper with the administrative account;

- Administrative accounts will not be used to install any software that has not been purchased by the University, or that has a licensing agreement allowing for free use at a University;

- Administrative accounts will not be used to install applications that may establish network share protocols which result in an increase in bandwidth utilization as this may cause network congestion and degradation of network performance across wide areas of the campus. Examples include peer-to-peer (P2P) applications such as BitTorrent, Gnutella, etc.;

- Administrative account users will allow for the removal of **any** software that adversely affects system efficiency or introduces a significant risk to system security as determined by UTech.

2. Scope of Administrative Accounts
   Faculty administrative accounts will work on the computer assigned to the individual and the instructor computers in each classroom. Faculty should login with their standard Active Directory account and use the "Run As" feature to make software changes. Logging into a workstation with an administrative account will not map file shares or allow for an email connection using the Outlook client.

3. Java Warning
   One of the most common software updates is the Java plugin. Certain applications, like Banner and D2L are only compatible with specific versions of Java. Updating Java to newer versions may prevent users from accessing Banner and D2L. As such, Java should only be updated by UTech.

4. Additional Warnings
   - Commercial computer software is protected by federal copyright laws. Individuals who download or install applications (software), other than those included in the standard configuration for all university computers, are responsible for retaining documentation of appropriate licenses.

   - Individuals are also responsible for re-installing this non-standard software if necessary.

   - Individuals are responsible for notifying the University of any software or modifications made to laptop configurations that might violate Export Control Laws when doing International travel.

   - Non-standard software will be removed as part of a normal repair process if necessary to restore system functionality.

5. Non-Compliance and Sanctions
   - Persons in violation of this directive are subject to the full range of sanctions, including without limitation the loss of access privileges to Resources, disciplinary action, dismissal from the University, and legal action. Some violations may constitute criminal offenses, as outlined by federal, Pennsylvania and all other applicable laws; the University will carry out its responsibility to report such violations to the appropriate

authorities. Violations of licensing policies may result in fines to individuals and/or departments.

D. **Effective date:** September 1, 2015

Adopted: September 1, 2015 **by:** President's Cabinet

Amended Date: