1.0 Purpose
This policy provides guidelines for appropriate user account privilege settings used during normal computer operations.

Computer security is the primary driving force behind this policy. In recent years, hackers have significantly increased their ability to compromise systems, making these systems participants in illicit activities or resulting in them being vulnerable to harvesting of institutional data or intellectual property. Most programs (of particular concern are web browsers) run at the same privilege level as the active user account. Even a well maintained system might be vulnerable to recently developed attacks. If the program is running with administrative level permissions, the compromise potentially has unfettered access to all system files and system resources.

2.0 Scope
This policy applies to all computer systems that meet any of the following criteria:

- Any computer system connected to the wired College of Engineering network
- College of Engineering owned computer systems
- Non-College of Engineering owned computer systems that hold College of Engineering institutional data.

This policy applies to all types of computers including but not limited to desktop computers, laptop/tablet computers, and servers.

3.0 Policy
All accounts used for normal login and computer operation must run at the lowest privilege setting (Least User Privilege) that still permits regular tasks to be accomplished. These accounts must NOT have administrative level privileges.

Administrative rights are normally restricted to the IT professionals entrusted to maintain the software, patches, and security of the system, unless an administrative exception is granted (see Administrative Accounts).

4.0 Administrative Accounts
Software installation/removal, patch management, and system configuration comprise the majority of computing activities that may occasionally require administrative access. In general this access is restricted to the IT professionals responsible for system management.

Exceptions: Maintenance, such as patch management falls under the duties and responsibilities of the IT professionals and is usually not a valid reason to be given administrative rights. Additionally, software installation needs to be properly vetted and also falls under the responsibilities of the IT professionals and is not usually a valid reason for requiring administrative or sudo rights. There are some instances where administrative rights may be required. These may involve extended travel, software development, etc. In those cases, users who need administrative or sudo access to a system must work with the IT staff responsible for the system to apply for administrative rights. The firewall exception/administrative rights committee will rule on the validity of the request. In most cases where administrative access is approved, that access will be provided by means of a College managed privilege escalation program, rather than a local administrative account.

Password Requirements: In the case that a local administrative account is authorized, those accounts must have complex, unique passwords that, according to College of Engineering policy, expire every 90 days. Additionally,
administrative accounts should be prevented direct logon to systems whenever possible, instead using “run as” (Windows) or sudo (Linux/Unix/OS X) for temporary privilege escalation.

Users who have demonstrated a legitimate need for occasional utilization of administrative access to a system must ensure that any utilization of an administrative level account or privilege escalation software be limited to system maintenance activities or software installation, and then only when elevated account rights are absolutely necessary to accomplish the task at hand.

5.0 Enforcement
Violation of this policy may result in termination of network access. Furthermore, any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

6.0 Definitions

<table>
<thead>
<tr>
<th>Terms</th>
<th>Definitions</th>
</tr>
</thead>
<tbody>
<tr>
<td>Administrative Level Privileges</td>
<td>The highest level of permission that can be granted to a computer user. This level of permission normally allows the user to install software that must be able to change system settings, manage the system, and change configuration settings.</td>
</tr>
<tr>
<td>Privilege escalation software</td>
<td>A program that elevates the privilege level of a program or group of programs above that of the user.</td>
</tr>
<tr>
<td>Sudo</td>
<td>A program for Unix-like computer operating systems that allows users to run programs with the security privileges of another user, including the superuser.</td>
</tr>
</tbody>
</table>

7.0 Frequently Asked Questions

What if I’m traveling and need to install software or make a system change?
You can connect to the VPN to access trusted install points where your vetted software resides. Privilege escalation software can elevate your access to allow that software to be installed from that trusted location. Additional rules can be applied to your system to allow you to make other approved changes as you’re connected to the VPN.

What if I have a program that just needs more access than I have as a typical user?
Most applications run perfectly for user accounts. Some may require Power User, which can easily be configured on your system. Any additional access requires the use of privilege escalation software.

How does privilege escalation software work?
An agent runs on your system that constantly monitors for processes that require elevated access. When that happens it checks against a predefined list of policies. If there is a rule match, the agent transparently elevates the process even though the user is still running with Least User Privilege.

How do I apply for an exemption?
A COE website will be available for anyone requiring special elevation rules or administrative access. Once you fill out an exception request, a committee will review it and either approve the request or suggest an alternative.

8.0 Revision Date
Last updated: 1/5/2016