Acceptable Computer Use Policy
COE–AUP–AD20

1.0 Purpose
The purpose of this policy is to outline the acceptable use of computer equipment within the College of Engineering. Inappropriate computer use exposes everyone to risks including virus attacks, compromise of network systems and services, and possible litigation. College computing systems are for business purposes in serving the administrative, academic and research activities of the College, University, faculty, staff and students.

Effective security is a team effort involving the participation and support of every College of Engineering employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines and conduct their activities accordingly.

2.0 Scope
This policy applies to faculty, staff, students, contractors, consultants, temporaries, and other workers in the College of Engineering, including all personnel affiliated with third parties. This policy applies to all equipment that is connected to the College of Engineering network.

3.0 Policy
3.1 General Use and Ownership
1. For security and network maintenance purposes, authorized individuals within the College of Engineering may monitor equipment, systems and network traffic at any time, per the College of Engineering’s Audit Policy.
2. The College of Engineering reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy and University policies.

3.2 Security and Proprietary Information
1. Systems must adhere to all of the University and College policies including requirements for protecting data based on the classifications set forth in the College’s Data Classification Standards and Security Requirements such as the possibility of requiring data be housed on an encrypted drive, and so forth. Please refer to the College of Engineering Data Classification Standards and Security Requirements policy to see what security measures are necessary to prevent unauthorized access to information.
2. All PCs, laptops and workstations should be secured with passwords for all local accounts in compliance with the College of Engineering’s Password Policy. Use additional settings as deemed necessary to prevent unauthorized access to resources and data that resides either locally or remotely. Additional security measures may be required based on the class of data being processed or housed on the system as mentioned in 1 above.
3. Passwords must be kept secure and accounts must not be shared. Authorized users are responsible for the security of their passwords and accounts. In addition to the password requirements listed in the College of Engineering Password Policy, it is strongly recommended that system level passwords should be changed quarterly, and user level passwords should be changed every six months.
4. All PC’s laptops and workstations must be routinely operated in Least Privilege User Account mode as outlined in the College of Engineering Least User Privilege Policy COE–LUP–01
5. All PCs, laptops and workstations that have security logging capabilities must have basic OS level auditing turned on to facilitate tracking of user accounts in the event of a security breach or other unauthorized access.
6. Because information contained on portable and remote computers is especially vulnerable, special care must be exercised. Portable systems containing sensitive university data should utilize hard drive encryption techniques to protect the data in the event of unauthorized physical access to the system. Portable systems often contain offline versions of internal restricted University data and must adhere to all requirements based on the classification of data residing on the system. Please refer to the College’s Data Classification Standards and Security Requirements Policy for more information.
7. While it is currently not required, postings by employees from a College of Engineering email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of The College of Engineering or the University, unless posting is in the course of business duties.

8. All computers used by the employee that are connected to the College of Engineering Internet/Intranet/Extranet, whether owned by the employee or the College of Engineering, should be continually executing approved virus-scanning software with a current virus database. These systems should be fully patched with all operating system patches as well as security patches for installed applications.

9. Employees must use extreme caution when opening unsolicited e-mail attachments, which may contain viruses, e-mail bombs, or Trojan horse code.

10. All systems connected with the College of Engineering’s network infrastructure may only use IP addresses assigned by the College or its delegates. Any departments providing IP addresses via DHCP must employ a mechanism to ensure that only the intended host receives the IP address or are authenticated and logged so that the user of that IP address during a given period of time can be determined in the event of a security incident.

11. To maintain proper data encryption, all systems storing or utilizing sensitive administrative data, and using a wireless connection must also utilize a College approved VPN (virtual private network) or WPA (WiFi Protected Access). Systems transferring sensitive university data over non-secure networks (wired or wireless) must encrypt that data during transmission.

3.3. Unacceptable Use
The following activities are prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services).

Under no circumstances is an employee of the College of Engineering authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing College of Engineering-owned resources.

The lists of prohibited activities presented below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or entity protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the College of Engineering.

2. Unauthorized copying or distribution of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted movies or music, and the installation of any copyrighted software for which the College of Engineering or the end user does not have an active license is strictly prohibited. Copying or distribution includes but is not limited to the utilization of peer to peer sharing software, downloads from or uploads to internet sites, email, or scanning, to acquire or distribute copyrighted material without documented authorization from the copyright holder.

3. It is illegal to export software, technical information, encryption software or technology, in violation of international or regional export control laws. The appropriate College security officer should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home. As an employee of the College and University, anyone who allows others to use College/University computing assets is responsible for any violation of federal and state laws and such incidents will be adjudicated by the University Security Office and the Office of Human Resources.

6. Using a College of Engineering computing asset to engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
7. Making fraudulent offers of products, items, or services originating from any College of Engineering account. Or, offers of products, items, or services for personal profit from any College of Engineering account.
8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access. The only exception to this is when access is part of a security analysis performed by an authorized individual within the College or University. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information.
10. Port scanning or security scanning is expressly prohibited unless prior approval is obtained from the College Network Security office.
11. Executing any form of network monitoring which intercepts data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
12. Circumventing user authentication or security of any host, network or account apart from assigned duties performed by IT professionals.
13. Interfering with or unsanctioned denying of service to any user other than the employee's host (for example, denial of service attack).
14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet apart from assigned duties performed by IT professionals.
15. Providing information about, or lists of, the College of Engineering employees to parties outside the University.

**Email and Communications Activities**

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through content, language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters" or "pyramid" schemes of any type.
6. Use of unsolicited email originating from within the College of Engineering's networks or other Intranet/Internet/Extranet service providers on behalf of, or to advertise, any service hosted by the College of Engineering or connected via the College of Engineering's network.
7. Posting identical or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

**4.0 Enforcement**

Any employee found to have violated this policy may be subject to disciplinary action by their Administrative unit, the College, or the University.

**5.0 Definitions**

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spam</td>
<td>Unauthorized and/or unsolicited electronic mass mailings.</td>
</tr>
<tr>
<td>Internet</td>
<td>A worldwide system of computer networks</td>
</tr>
<tr>
<td>Intranet</td>
<td>A private network that is contained within an enterprise.</td>
</tr>
<tr>
<td>Extranet</td>
<td>A private network that uses the Internet protocol and the public telecommunication system to securely share part of a business's information or operations with suppliers, vendors, partners, customers, or other businesses.</td>
</tr>
</tbody>
</table>

**6.0 Revision History**

Last updated: 12/17/2009