

**College of Engineering Acceptable IT Use Policy (EGR AUP)
Division of Engineering Computing Services (DECS)
2007**

All College of Engineering faculty, staff, visiting scholars, graduate students, undergraduate students and guests with a valid engineering account may use engineering computer systems, network, and other technology and resources. The use of engineering and MSU computing systems, software, and networks is a privilege which requires following the guidelines outlined in this document.

All engineering students and students enrolled in engineering classes are provided an engineering account (EGR NetID) which gives access to the resources provided for the students by the College of Engineering. This is separate and in addition to the MSU NetID. When an engineering student graduates or is no longer enrolled in engineering classes, the engineering student's account will expire on the 15th of the month following the beginning of the next semester.

It is the responsibility of every person with an EGR NetID to read and abide by the policies outlined in this document and MSU's Acceptable Use of Computing Systems, Software, and the University Digital Network Policy <http://www.msu.edu/aup>.

In this document, the term "computing infrastructure" encompasses computers, computer networks, connections to external computer networks, software, e-mail, User data, web site/pages, all peripherals, and all information resources. "User" is the person to whom an engineering EGR NetID has been assigned. "User Data" is any format of information and/or multimedia, including e-mail and web site content.

The College of Engineering Acceptable IT Use Policy (EGR AUP) outlines the responsible use of all computing facilities, as well as the rights and responsibilities of Users. Violations of these policies are subject to the same treatment as violations of any college or university policy which can result in the loss of a User's EGR NetID, the loss of a User's MSU NetID, and disciplinary actions as determined by the university.

- Users may not transfer account privileges to another individual. An EGR NetID is assigned to an individual. The authorized User is responsible for the proper use of the account, computer facilities and resources including password protection and file access and permissions. The User is responsible for all actions made under this account. **Sharing your account**

or giving access to your account to another user is prohibited and will result in the loss of your account and access to all resources.

- Each user should understand how to protect personal information and take the steps necessary to protect that information. It is stressed that every User protects personal data and information, password, and Internet identity as much as to his/her ability to do so. Any attempt by a User to gain any unauthorized access to private information will be considered a violation of privacy. Access of that information without authorization from the owner is a violation of a Users rights. Every User should understand how to **protect personal information, identity, and sensitive data** and to take the steps necessary to protect that information.
- It is important for all users to understand what type of information is stored. This applies to researchers, administrators – anyone working with or collecting information which could potentially violate the privacy and rights of others, particularly **FERPA** (<http://www.reg.msu.edu/ROinfo/Notices/PrivacyGuidelines.asp>)
- Mailboxes, web space, a User's home space, a User's personal data and information, research software and data, database content, even data stored in public areas should be treated as being private. Although a User may inadvertently not enforce the appropriate protection, this does not mean that others may assume that it is permissible to access or inspect information or data belonging to another user. Information about a User which might be visible to others (usernames, e-mail address, etc.) and which might not be secure should not be used to harass, monitor, or stalk the User or in any way intrude on the User's right to privacy.
- Request for another User's files (data/e-mail) will be denied, unless written permission from the owner of the files (the User) is obtained and provided.
- The College of Engineering does not censor materials or opinions on its systems. However, e-mail must not be obscene or harassing and messages must not misrepresent the identity of the sender.
- Adhere to copyright laws if copying or sharing any type of software, data, or other media.
- The use of resources for personal, commercial or private gain is prohibited.

- Software is under strict licensing agreements with the respective owner of the binary and source code. Any copying or remote use of software is prohibited unless otherwise stated. Illegal file sharing is prohibited. Any user involved in this activity will be subject to disciplinary actions as determined by the university.
- To protect yourself and others, laptops, tablets, mobile devices, desktops and servers **must** be free from viruses. Take precaution to ensure that personal equipment is properly protected and up-to-date with patches and malware protection software tools.
- Chain letters and mail SPAM will not be tolerated. Presenting false or misleading information, deliberately misrepresenting yourself on a web-page and any type of plagiarism is a serious violation of this and other policies and may be referred to the appropriate university committee for resolution.
- Theft, rearrangement or damage to any computer or network equipment is strictly prohibited and will be reported to campus police. This includes all public computer labs.

DECS reserves the right to deny access to any user violating this policy, as well as reporting the incident to the Vice Provost for Libraries, Computing and Technology. The College of Engineering reserves the right to amend this document at any time, with or without notice.