Campus Network Connection and Acceptable Use Policy

Academic Computing and Networking

Updated: August 12th 2007

Computing and data communications resources at the Colorado School of Mines are valuable and limited resources that serve a large number and variety of users. All users have the responsibility to make use of these resources in an efficient, ethical, and legal manner.

The School's computer and network services provide access to resources on and off campus and shall be used in a manner consistent with the instructional, research, and administrative objectives of the School and with the purpose for which such use was intended. Such open access is a privilege, and imposes upon users certain responsibilities and obligations. Access to the School's network services is granted subject to School policies, and local, state, and federal laws. Acceptable use is always ethical, reflects academic honesty, and shows restraint in the consumption of shared resources. It demonstrates respect for intellectual property, ownership of data, copyright laws, system security mechanisms, and individuals' rights to privacy and to freedom from intimidation and harassment. All activities inconsistent with these objectives are considered to be inappropriate and may jeopardize continued use of computing facilities and networks.

In consideration of being allowed to use the School's network resources, users acknowledge and agree to the following:

1. I shall not use network resources for any illegal activity or for any activity prohibited by this policy (see subsequent pages for examples of inappropriate conduct that is prohibited), the "Computing & Networking Resource and Responsible Use Policy", the Standards and Codes of Conduct (see http://www.is.mines.edu/FO/SRTK/rules.shtm) or the policies set forth in the Faculty Handbook (see http://www.mines.edu/Academic/affairs/fachandbook/).

2. I agree not to use network resources to infringe upon or otherwise impair, interfere with or violate any copyright or other intellectual property rights of another. This pertains to all copyrighted material, including, but not limited to music, video and software. I understand that I may be potentially liable for misuse of the Resources, including acts that are contrary to school policy. Except for such claims as may be covered by the Governmental Immunity Act (Colorado Revised Statutes 24-10-101 et seq.), I agree to be responsible for all claims arising from my misuse of the network and shall indemnify and hold harmless CSM from any costs, expenses or liabilities that might be asserted or imposed upon it or any of its officers, agents or affiliates as a result of such misuse.

3. I shall avoid any action that interferes with the efficient operation of the network or impedes the flow of information necessary for academic or administrative operations of the School.

4. I shall protect my computer resources such as EKey, logins and systems from unauthorized use. I acknowledge that I am responsible for reasonably securing my computer, including implementing such protections as logins to prohibit unauthorized use, applying in a timely fashion operating system and software patches that protect my computer from hackers, and implementing virus scanning software.

5. I will access only information that is my own, which is publicly available, or to which I have been given authorized access.

6. I will not make use of the network, even through a personally owned computer, for financial gain (personal or commercial) without the express written consent of the School.

Examples of Inappropriate Conduct:

- Installation and use of any wireless router, base-station or any other device that may interfere with the School's wireless network.
- Uploading or downloading of any copyrighted material, including music and video, to which you do not have a right to access or distribute.
- Attempting to "sniff" the network or capture transmissions bound for other systems
- Accessing another person's computer, computer account, files, or data without permission.
- Attempting to circumvent or subvert system or network security measures. Examples include creating or running programs that are designed to identify security loopholes, to decrypt intentionally secured data, or to gain unauthorized access to any system.
- Harassing or intimidating others via electronic mail, news groups or Web pages.
- Providing access to others through a personal account or sharing access codes with roommates, friends, or even family, violates policy and can lead to disciplinary action. Each individual is responsible for activity or transmissions that originate from a personal account or computer.
- Initiating or propagating electronic chain letters.
- Initiating or facilitating in any way mass unsolicited and unofficial electronic mailing (e.g., "spamming", "flooding", or "bombing.").
- Forging the identity of a user or machine in an electronic communication.
- Saturating network or computer resources to the exclusion of another's use, for example, overloading the network with traffic such as emails or legitimate (file backup or archive) or malicious (denial of service attack) activities.
- Using the School's systems or networks for personal gain; for example, by selling access to your eKey or to school systems or networks, or by performing work for profit with school resources in a manner not authorized by the School.
- Engaging in any other activity that does not comply with the general principles presented above.

Enforcement

The School considers violations of acceptable use principles or guidelines to be serious offenses. The School will take such action it deems necessary to copy and examine any files or information resident on school systems allegedly related to unacceptable use, and to protect its network from systems and events that threaten or degrade operations. Violations may be referred to the appropriate school entity for discipline.

Academic Computing and Networking will use its best efforts to contact the offending party via email, telephone, or in person to explain the problem and discuss its resolution before taking any action deemed necessary to protect the integrity of the Resources. In the case of major infractions, for example those that impair others' ability to use networking and computing resources, Academic Computing and Networking Services may immediately restrict systems or network access as it deems necessary to mitigate such activities. Only thereafter will Academic Computing and Networking Services make a reasonable effort to contact the involved parties when these incidents occur.

Note that while the School takes the privacy of our students seriously, E-mail, disk files, and network transmissions, though protected by security mechanisms, are not private. They may be examined by Computing Center staff to evaluate system or network or load problems or for some similar reason, or if there is reason to believe that accounts or systems have been compromised or involved in a violation of policy or law.

HISTORY AND REVIEW CYCLE

The policy will be reviewed at least annually, or as needed by the Responsible Administrative Unit.
Last Issued: August 2007