	Information Technology Appropriate Use Policy	**Responsible Administrative Unit:** Computing, Communications & Information Technologies
	Issued: March, 2014 **Revised:**	**Policy Contact:** Chief Information Officer

1.0 BACKGROUND AND PURPOSE

Information Technology ("IT") includes a vast and growing array of computing, electronic and voice communications facilities and services. At the Colorado School of Mines ("Mines" or "the school"), IT plays an integral role in the fulfillment of the school's research and educational missions and on-going administrative operations. Taxpayers, students, other funding sources, and the public at large, expect that these assets will be used in a lawful manner to effectively and efficiently support the school's mission. Users of Mines' IT assets have a responsibility not to abuse them and to respect the rights of other members of the Mines' community as well as the school itself. The following policy provides for the appropriate use of Mines' IT systems.

2.0 SCOPE

2.1. Applicability: This policy applies to all users of Mines' IT systems including, but not limited to, Mines students, faculty, staff, guests, contractors, and visitors. It applies to the use of all Mines' IT systems including systems, networks, and facilities administered by the Department of Campus Computing, Communications, and Information Technologies (CCIT), as well as those administered by individual departments, laboratories, and other Mines units. This policy also covers systems not owned or managed by Mines under certain conditions of law related to public records, copyright, and others, especially if those systems are associated with the school and periodically connected to it via networking facilities.

2.2. Existing Policies. Policies that already govern facilities use, freedom of expression, academic integrity, privacy, electronic mail, electronic communications with students and employees, sexual harassment, and others, may apply to IT Systems use as well. This Policy addresses circumstances which are more directly IT related and is intended to augment, not supersede, any other relevant school policies. (see Section 4.7)

2.3. Detailed Appropriate Use. Faculty, staff, and students must be aware of their department or office policies and governing documents concerning appropriate use. These documents may contain more detailed statements regarding appropriate use. Such statements may be more restrictive than this policy, but may not be more permissive. In the event of a conflict, this Information Technology Appropriate Use Policy will prevail.

3.0 POLICY

The Colorado School of Mines seeks to provide for the following:

- An IT infrastructure which promotes and facilitates the educational and research missions of Mines as well as its administrative functions;
- IT systems which are reliable, available, and perform in a superior manner.

In order to facilitate these goals, IT systems may only be used for their intended purposes, as authorized, in support of the research, educational, administrative, and other appropriate functions of Mines. Users are expected to exercise good judgment and operate under best practices in the

use of IT systems. All users have an ethical and a legal responsibility to use IT systems appropriately and will be held accountable for their behavior.

4.0 SPECIFIC PROHIBITIONS

The following categories of IT systems use are prohibited:

4.1. Use that interferes with, stops, impedes, or impairs the intended use of an IT System, or otherwise causes harm to the activities of others. Users shall not deny or interfere with (or attempt to deny or interfere with) the operation of an IT System or impair service to other users in any way. This includes any form of "monopolization", misusing mailing lists, propagating chain letters or virus hoaxes, "spamming" (spreading email, postings, instant messages, etc., widely and without good purpose), etc. These acts (or examples), or any other behaviors which may cause excessive network traffic or computing load are prohibited.

4.2. Use for commercial personal gain. Mines IT resources are provided to students primarily to fulfill their academic responsibilities and obligations and to employees to fulfill their professional responsibilities. Students shall not use Mines IT resources to operate a business or for ongoing commercial activity that generates personal income. Employees shall not use Mines IT resources to operate a business or for consulting or commercial activity that generates personal income or financial gain. Certain exceptions to this restriction may exist. Rules and procedures identified in the Faculty Handbook, emeritus, separation, or similar agreements with the institution will determine and govern these exceptions.

4.3. Harassing or threatening use. Users shall not utilize IT systems such as e-mail or messaging services to harass or intimidate another person. Two examples include sending repeated unwanted mail and display of material known to be offensive to others (e.g. sexual material.)

4.4. Use which damages the integrity of the school or of other IT systems. Examples in this category include the following:

4.4.1. ***Attempts to defeat system security.*** (e.g. by "cracking" or guessing credentials, compromising room locks or alarm systems, etc.) This provision does not prohibit CCIT or authorized systems administrators from using appropriate tools within the scope of their job responsibilities and authority.

4.4.2. ***Unauthorized Access or Use.*** Users may only use the IT Systems they are authorized to use and only for the purposes specified when their authorization was granted. Specifically:

i. Users may not seek or assist others in seeking access to IT systems or to data on IT Systems that they are not authorized to access.

ii. Users may not use other's system credentials or allow others to use their credentials under any circumstances.

iii. Users shall not intercept or access data communications (or attempt to intercept or access data communications) that are not intended for them.

iv. Users shall not make or attempt to make any deliberate, unauthorized data changes on any IT system.

v. Users shall not utilize or attempt to utilize any IT system to detect, attack, or exploit weaknesses in any other systems, on or off-campus.

vi. Users shall not access data elements, even if coincidentally authorized, which are not required for the purposes specified in their authorization or, for employees, for purposes not required by their job duties (e.g. accessing data out of simple curiosity.)

4.4.3. ***Disguised use.*** Users shall not conceal their identity when using IT systems unless the option of anonymous access is explicitly authorized. Users also shall not masquerade or impersonate another person or otherwise use or attempt to use a false identity in any way.

4.4.4. ***Violations of Privacy or Confidentiality.*** Whether done intentionally or not, users shall not disclose private, legally protected, or other sensitive personal information concerning a member of the Mines community, or disclose any other confidential information to which they have access, either publicly or to another individual who is not authorized to access the same information. In the event of an unintentional disclosure of personal or sensitive information users are expected to notify the CISO immediately.

4.4.5. ***Distribution of "malware."*** Users shall not knowingly distribute or launch computer viruses, worms, or other "malware."

4.4.6. ***Removal or modification of data or equipment.*** Without specific authorization, Users shall not remove or modify any school-owned or administered equipment or data from IT systems.

4.4.7. ***Use of unauthorized devices.*** Users shall not attach network switches, routers, wireless access points, or any other device to the campus network without authorization and proper registration. Users shall not permanently attach (physically or electronically) additional devices to IT systems managed by CCIT without authorization. Temporarily connected devices such as USB flash drives must comply with all applicable IT, data management, and security policies.

4.5. Use in violation of law. Illegal use of IT systems is prohibited. Illegal use means use in violation of applicable civil or criminal law at the federal, state, or local levels. Examples include: distributing, receiving, transmitting, or possessing child pornography; infringing upon any copyright, trademark, or patent; etc.

4.5.1. Compliance With Copyright Law Use of school information systems must comply with provisions of copyright law and fair use. Copyright law limits the rights of a user to decrypt, copy, edit, transmit or retransmit another's intellectual property, including

written materials, images, sounds, music, and performances, even in an educational context, without permission, except where such use is in compliance with Fair Use or TEACH Act provisions.

4.6. Use in violation of school contracts. All use of IT systems shall be in compliance with Mines' contractual obligations to software vendors, research granting agencies, and any other licensing agreements.

4.7. Use in violation of school policy. Use of IT Systems which violates other school policies also violates this policy. See Section 2.2.

4.8. Use in violation of external data network policies. Users shall observe all applicable policies of external data networks when using such networks.

Please note that this list of specific prohibitions is not exhaustive. With the rapid advancement of IT systems technology, other inappropriate uses may develop that are not listed above. The school reserves the right to investigate any complaints or suspicion of alleged abuse of IT systems regardless of its inclusion in this section.

5.0 RESPONSIBILITIES

5.1 Personal Account Responsibility. Users are responsible for maintaining the security of their IT Systems accounts and passwords. Accounts and passwords may not be shared with others. Users are responsible for any activity carried out under their IT Systems accounts.

5.2 Incidental Personal Use. Incidental personal use is an accepted and appropriate benefit of being associated with Colorado School of Mines technology environment. Appropriate incidental personal use of technology resources does not result in any measurable cost to the school, and benefits the school by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable school policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's school responsibilities, or adversely impact or conflict with activities supporting the mission of the school. Note that any files stored on Mines resources are considered property of the school and subject to all school, state and federal regulations including the Colorado Open Records Act.

5.3 Encryption of Data. All data that belongs to the Colorado School of Mines that is stored on any mobile device, and disclosure of which poses a security risk, must be encrypted using an institutionally approved encryption application. Further information is available in the *Administrative Data Policy, Mandatory Use of Encryption Software for Mobile Devices* executive directive, and the *Security Practices and Guidelines* document.

5.4 Responsibility for Content. Official school information may be published in a variety of electronic forms. The certifying authority under whose auspices the information is published is responsible for the content of the published document.

Users also are able to publish information on IT systems or over Mines' networks. Neither Mines nor CCIT can screen such privately published material nor can they ensure its accuracy or assume responsibility for its content.

5.5 Content Security. The school takes reasonable steps to promote and preserve the security of its IT systems, yet security can be breached through actions beyond the school's reasonable control. Therefore, the school cannot guarantee the absolute security of any user's content. Further, the school relies on users to employ reasonable means to protect their own security and thereby, that of the entire IT Systems environment. (See Section 4.)

5.6 Content Privacy. The school takes reasonable steps to promote and preserve the privacy of its IT systems, yet privacy can be breached through actions beyond the school's reasonable control. Further, while not a breach of privacy, but rather as part of their routine job duties, users should be aware that systems administrators may coincidentally come into contact with user's content or may even be required to analyze that content or its metadata to support IT system integrity.

5.7 IT System Logs. IT systems routinely log user actions in order to facilitate recovery from system malfunctions or for other appropriate IT system management purposes. Users should recognize that the extent of individually identifiable data collected in IT systems logs may vary.

5.8 Personal Identification. Upon request of a systems administrator or other school authority, users shall produce valid Mines identification (e.g. when requesting access to a secure IT system or area.)

6.0 ENFORCEMENT PROCEDURES & PENALTIES

6.1 Complaints of Alleged Violations. An individual who believes that he or she has been harmed by an alleged violation of this policy may file a complaint in accordance with established grievance procedures for students, faculty, and staff, including procedures for filing sexual harassment complaints, when relevant. The individual is also encouraged to report the alleged violation to the systems authority overseeing the facility most directly involved, or to the Chief Information Security Officer ("CISO"), or to the Chief Information Officer ("CIO").

6.2 Reporting Observed Violations. An individual (including a CCIT employee) who believes that he or she has observed or otherwise is aware of a violation of this policy but has not been harmed by the alleged violation shall report the violation to the systems authority overseeing the facility most directly involved, or to the CISO, or to the CIO.

6.3 Disciplinary Procedures. Alleged violations of this policy will be pursued in accordance with the appropriate disciplinary procedures for faculty, staff, and students, as outlined in the Faculty Handbook, State Personnel Rules, Student Handbook Policies, and other applicable law and materials. CCIT will assist as required in these procedures.

6.4 Penalties. Violators of this policy may be subject to penalties provided by the applicable procedures and policies referenced in the preceding paragraph, as well as IT-specific penalties including temporary or permanent reduction or elimination of some or all IT privileges, and any penalties established by applicable law. The appropriate penalties shall be determined by the applicable disciplinary authority in consultation with the CIO. Further, the school, acting through an authorized systems administrator, may deactivate a user's IT privileges any time it deems deactivation necessary to preserve the integrity and/or safety of facilities, user services, data, or other assets.

6.5 Legal Liability for Unlawful Use. In addition to school discipline, users may be subject to criminal prosecution, civil liability, or both, for any unlawful use of any IT system.

6.6 Appeals. Users found in violation of this policy may use the appeals process defined in the relevant disciplinary procedure applied to the incident.

7.0 DEFINITIONS:

7.1 IT Systems: The computers, terminals, printers, network and other appliances, wiring infrastructure, telephone and telecommunications devices and software, online and offline data storage media and related equipment, owned or licensed software, applications, and data files owned, managed, or maintained by the school. These include institutional as well as departmental information systems, faculty research systems, desktop computers, Mines campus data and telecommunications networks, general access computer clusters, etc.

7.2 Malware: Any one of a variety of forms of hostile, intrusive, or annoying software or program code designed to infiltrate a computer system without the owner or user's intent. Malware includes computer viruses, worms, trojan horses, spyware, dishonest adware, crime-ware, most rootkits, and other malicious and unwanted software. Malware is not the same as defective software or software that has a legitimate purpose but contains harmful bugs.

7.3 User: A "user" is a person who makes use of any Mines IT system from any location, whether that use is authorized or not. For example, users include a person using an on-campus cluster computer as well as a person using his or her own personal computer off-campus but connected to a Mines' IT system via network.

7.4 Systems Authority: Mines as the legal owner and operator of all of its IT systems, delegates oversight of particular systems to the head of a specific subdivision, department, or office of the school, or to an individual faculty member in particular cases including those IT systems purchased with research or other funds for which the faculty member is responsible. The individual with delegated oversight of an IT system is the System Authority and is responsible for all aspects of that system.

7.5 Systems Administrator: Systems Authorities often designate one or more persons as "System Administrator(s)" to manage the particular IT system(s) assigned to them. System Administrators oversee the day-to-day operation of the system including provision of authorized user credentials.

7.6 Certifying Authority: An employee of the school who has been given the authority to certify the appropriateness and accuracy of an official school document for electronic publication in the course of school business, such as the Director of Public Relations, Registrar, the Director of Institutional Research and/or other authorities who are responsible for publications.

7.7 Specific Authorization: Documented permission (e.g. an approved system access request form or other valid communication on file, or a valid Mines e-Key) to use a specific IT System for a specific purpose granted by the systems authority, system owner, the CIO or the responsible Vice President in their respective area.

8.0 POLICY REVIEW:

This policy may be periodically reviewed by the CIO who may consult with relevant school committees, faculty, students, and staff regarding changes that should be considered.