	Information Technology Appropriate Use Policy	
	Responsible Administrative Unit: Information Technology (IT)	**Policy Contact:** Office of the CIO, ocio@mines.edu

1.0 BACKGROUND AND PURPOSE

Information Technology (IT) resources include 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 resources and assets will be used in a lawful manner to effectively and efficiently support the school's mission. Users of Mines' IT resources and 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 resources.

2.0 SCOPE

2.1. Applicability: This policy applies to all users of Mines' IT resources including, but not limited to, Mines students, faculty, staff, guests, contractors, and visitors. This policy applies to the use of all Mines' IT resources including systems, networks, applications, data, and facilities administered by IT, as well as those administered by individual departments, laboratories, and other Mines units. This policy also covers technology resources not owned or managed by Mines under certain conditions of law related to public records, copyright, and others, especially if those resources are associated with the school.

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

To facilitate these goals, IT resources 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 proper judgment and operate under best practices in the use of IT resources. All users have an ethical and a legal responsibility to use IT resources appropriately and will be held accountable for their behavior.

Users are responsible for the security of data, accounts, and systems, and other assets under the user's control. Users shall keep passwords secure and not share account or password information with anyone, including family, friends, or other Mines personnel. Providing access to another individual, either deliberately or through failure to secure its access, is a violation of this policy.

The Internet and other network access is provided for business use. Occasional personal use is expected but excessive or inappropriate personal use is not acceptable. Mines reserves the rights to monitor Internet and network use, including the identity and content of sites visited, pages viewed, or files downloaded with any Internet browser, or any other access software, and to restrict or revoke a user's Internet or other networks access privileges.

Mines may override individual credentials and access Mines owned resources at any time. Communications and data on Mines technology resources are not private or confidential. Mines retains the right to retrieve, read and publish any communications or data placed on Mines technology resources. Deletion of communications or data by individuals does not necessarily remove such messages from the technology resource and, in some cases, deleted communications and data may still be accessed after deletion by an individual user. Accordingly, as with all business communications, use of technology resources should be prudent and professional.

4.0 SPECIFIC PROHIBITIONS

The following categories of IT resource use are prohibited:

4.1. Use that interferes with, stops, impedes, or impairs the intended use of an IT System or other technology resources, 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 resource or impair service to other users in any way. This includes any form of "monopolization", misuse of communications resources, or the intentional or unintentional use of applications or other mechanisms for which the intended use is the generation of network traffic or other data for the purposes of overwhelming a technology resource for the purposes of

service disruption. These acts (or examples), or any other behaviors which may cause excessive network traffic or computing load are prohibited.

4.2. Use for commercial or 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 and shall be authorized for approval prior to undertaking. 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 resources such as communication platforms to harass or intimidate another person. Two examples include sending repeated unwanted email and display of material known to be offensive to others (e.g. sexually explicit material.)

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

4.4.1. ***Attempts to defeat system or other technology resource security.*** (e.g., attempting to gain unauthorized access to any technology resource, asset, or data through any means, or compromising physical security controls, etc.) This provision does not prohibit IT or authorized IT resource 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 resources 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 resources or to data on IT resources that they are not authorized to access.

ii. Users may not use other's 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 resource.

v. Users shall not utilize or attempt to utilize any IT resource to detect, attack, or exploit weaknesses in any other technology resources, 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 Unauthorized use of technology communications resources for such purposes as soliciting or proselytizing for

commercial ventures, religious or personal causes or outside organizations or other similar, non-job-related solicitations is a violation of Mines policy and may result in discipline up to and including termination.

4.4.3. *Disguised use*. Users shall not conceal their identity when using IT resources 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, sensitive personal information, or other information deemed sensitive in nature by Mines, 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 office of Privacy immediately.

4.4.5. *Distribution of "malware."* Users shall not knowingly install, distribute, or launch malware in any form.

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

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 assets 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 resources 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 technology resources 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 resources 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. Mines users are prohibited from identifying themselves as Mines personnel or making any statement or representation on behalf of Mines in any electronic communication exchange except in the normal course of official Mines business. Use of IT resources 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 technology resources, 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 resources 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 resource accounts and passwords. Accounts and passwords may not be shared with others. Users are responsible for any activity carried out under their IT resource accounts. Users may be given passwords to access on-line databases that contain sensitive information from public records. Use of such databases and information is strictly for legitimate Mines business only. Users may not use Mines provided passwords or resources for personal reasons.

5.2 Incidental Personal Use. Incidental personal use is an accepted and appropriate benefit of being associated with the Colorado School of Mines technology environment. Appropriate incidental personal use of technology resources does not result in any measurable cost to the university and benefits the university by allowing personnel to avoid needless inconvenience. Incidental personal use must adhere to all applicable university policies. Under no circumstances may incidental personal use involve violations of the law, interfere with the fulfillment of an employee's university responsibilities, or adversely impact or conflict with activities supporting the mission of the school. Note that any data stored on Mines resources are considered property of the university and subject to all university, state and federal regulations including the Colorado Open Records Act. Mines reserves the rights to monitor use of technology resources including the Internet and other network resources, including the identity and content of sites visited, pages viewed, or files downloaded with any Internet browser, or any other access software, and to restrict or revoke a user's technology resource or Internet or network access privileges.

Devices supplied by Mines are provided for Mines business. Downloading, installing, and/or using applications or data except solely for Mines business, is prohibited. Installation of software not coordinated in advance and approved by the university is prohibited.

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 are also able to publish information on IT resources or over Mines' networks. Neither Mines nor IT 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 resources, 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 resource environment. (See Section 4.)

5.6 Content Privacy. The school takes reasonable steps to promote and preserve the privacy of its IT resources, 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 IT resource administrators may coincidentally encounter user's content or may even be required to analyze that content or its metadata to support IT system integrity. Users must lock the screen or log off any device when the device is unattended.

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

5.8 Personal Identification. Upon request of an IT resource administrator or other school authority, users shall produce valid Mines identification (e.g., when requesting access to a secure IT resource 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 resource authority overseeing the facility most directly involved, or to the senior information security practitioner for the university, or to the Chief Information Officer ("CIO").

6.2 Reporting Observed Violations. An individual (including an IT 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 technology resource authority overseeing the facility most directly involved, or to the senior information security practitioner for the university, 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. IT 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 IT resource 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 resource.

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:

IT Resource means infrastructure equipment, servers, terminals, end-user devices, printers, network and other appliances, wiring infrastructure, telephone and telecommunications devices and software, online and offline data storage media and applications, and related equipment, owned or licensed software, applications, databases, and data owned, managed, or maintained by the school. These include institutional as well as departmental information systems, faculty research systems, desktop and mobile computers, Mines campus data and telecommunications networks, general access computer clusters, etc.

Malware means any one of a variety of forms of hostile, intrusive, or annoying software or program code designed to infiltrate a computer system or other technology resource 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.

User means a person who makes use of any Mines IT resource 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.

Technology Authority means Mines as the legal owner and operator of all of its IT resources, may delegate oversight of resources 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 resources purchased with research or other funds for which the faculty member is responsible. The individual with delegated oversight of an IT resource is the System Authority and is responsible for all aspects of that resource.

IT Resource Administrator means Technology Authorities often designate one or more persons as "IT Resource Administrator(s)" to manage the IT resources(s) assigned to them. IT Resource Administrators oversee the day-to-day operation of the resource including provision of authorized user credentials.

Certifying Authority means 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.

Specific Authorization means 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 resource for a specific purpose granted by the resource authority, resource owner, the CIO or the responsible Vice President in their respective area.

9.0 HISTORY AND REVIEW CYCLE

The policy within this document will be reviewed no less than annually, or as needed by the Responsible Administrative Unit.

Issued: March 2014
Updated: January 26, 2024