	Required IT Security Practices and Guidelines	**Responsible Administrative Unit:** Computing, Communications & Information Technologies
	Issued: March, 2014 **Revised:**	**Policy Contact:** Chief Information Officer

1.0 BACKGROUND AND PURPOSE

The Colorado School of Mines' ("Mines", "the School", or "the Institution") information and technology (IT) systems, networks, and data are critical and valuable assets to the School and its mission. The purpose of these guidelines and required practices are to identify the procedures that Mines' community members must follow when using or accessing institutional resources or data.

2.0 SCOPE

All students, faculty, staff, affiliates, contractors, and guests who are provided with access to institutional data or other School IT resources including campus networks and access to the Internet are required to observe, implement, and follow the security procedures and practices listed below. These requirements also apply to personally-owned computers that connect to or through the campus network including over the VPN, as well as any system or device that accesses or stores institutional data. Some of the practices listed (such as strong password creation, password change requirements, OS and security updates) may be implemented in an automated fashion for certain groups of users or types of systems (computer labs, for example) using technology-based solutions.

Individuals who use CSM networks and IT resources are expected to familiarize themselves, and comply, with the responsibilities and practices listed below.

3.0 RESPONSIBILITIES AND REQUIRED PRACTICES AND PROCEDURES

Access to Server Rooms, MDFs, IDFs, and other Physical Infrastructure

- Restricted to personnel authorized by the CIO and/or CISO only.
- Server rooms shall be accessible only by logged electronic access except in a life safety emergency
- Electronic access to server rooms shall require two-factor authentication (access card + code entry)
- Server rooms shall be protected by recorded video surveillance systems
- Electronic access authorization lists shall be reviewed and updated at least quarterly
- MDFs, IDFs, and other infrastructure access locations shall be kept locked at all times. Contractors or staff are not to prop doors open when they are not physically present.

Wired and Wireless Network Connections and Access (including in Campus Housing)

- Only one device is to be connected per network jack. Network switches, wireless access points, routers and similar devices may not be installed by users unless explicit approval is received from CCIT. If unauthorized devices are detected, the network port will be deactivated and account access may be suspended.
- Hardware firewalls and Network Address Translation (NAT) devices may not be installed by users.
- Wireless access points may not be installed by users. If detected, the network port will be deactivated. This includes devices such as wireless printers that can act as an access point.
- Wireless-capable printers and disk drives are not to be used in wireless mode.
- Wired and wireless devices must be registered for use on the campus network.
- Domain Name Services (DNS) and Dynamic Host Configuration Protocol (DHCP) services are to be managed only by CCIT.
- Individuals, colleges, academic or administrative departments may not create, register, or support domain names appearing to represent the institution without authorization from CCIT.
- CCIT has the authority to implement Quality of Service technology to manage costs and insure the adequate performance and conduct of academic and administrative business of the institution.

Life Safety Systems and Applications

- Systems involving life-safety applications connected to the campus network must be on a physically or logically isolated network. Examples include fire alarms, environmental control devices, emergency phones, etc.
- Life-safety applications and related systems must undergo a thorough security review by CCIT and MEA.

Office Computers and Workstations

- Must run anti-virus, preferably provided by the institution.
- Must have operating system and security updates routinely applied.
- Must have application updates applied if they are security related.
- Should make use of centralized storage (typically H, I, Z, Y drives) – mandatory for administrative users.
- Must not store confidential or restricted institutional (as defined in the document *Data Classification and Roles Definitions*) data on local hard drives or mobile storage devices unless those drives or devices are protected by an authorized encryption method.
- Documents and data must be routinely backed up on a regular schedule, preferably to central backup systems. Backup guidelines and protocols can be found at *ccit.mines.edu/backups*
- Must have a password-protected screen saver turned on and set to15 minutes or less.
- Software applications must be appropriately licensed.
- May not host, distribute, or share copyrighted or protected content or software without proof of authorization.
- May not be configured to offer services to off-campus users.

Personally Owned Computers and Networked Devices Connected to the Campus Network

- Must run anti-virus and anti-malware software.
- Must have operating system and security updates routinely applied.
- May not be configured to offer services to off-campus users.
- May not download or store institutional data classified as restricted or confidential to local storage.
- Must operate using appropriately licensed software.
- May not host, distribute, or share copyrighted or protected content or software without proof of authorization.

Computer Teaching Labs, Classroom Podium Systems, and Related

- Systems are to be as "locked down" as possible to promote reliability and availability.
- Systems shall be configured to prevent and limit copyright infringement and installation of applications by users.
- Anti-theft alarms should be attached to appropriate devices.
- Software applications must be appropriately licensed. "Demo" software may not be installed for class use.

Laptops, Tablets, Smartphones

- Laptops purchased with any School funds must be encrypted as described in the executive directive titled *"Mandatory use of Encryption Software for Mobile Devices"*.
- Tablets or Smartphones containing any institutional data should be encrypted and protected by a passcode or other method. All Tablets or Smartphones shall have the user ID feature enabled and where appropriate, an enabled "find" or "wipe" feature as well.

Portable Storage Devices and Media

- Institutional data should not be routinely stored on portable media.
- If it is necessary to store institutional data on portable media, the files or entire device must be encrypted.

Encryption and Travel

- It is illegal to enter some countries with a laptop, device, or media that contains encrypted data. If you are traveling to one of these countries, you must have the encryption software removed and you must remove all institutional data classified as confidential and restricted from the device. Travelers are encouraged to borrow a laptop from CCIT and place only the data on it that you need for your trip.

Server Operations

- Should be centrally housed and managed where possible.
- Must be physically secured and protected.
- Be protected by a hardware-based firewall.
- Must run anti-virus and anti-malware software provided by the institution.
- Must have operating system and security updates routinely applied.
- Must have application updates applied if they are security related.
- Data stored on server must be backed up and retained according to backup/retention procedures.
- System activity logs are to be retained for 28 days.
- Must be disposed of according to equipment disposal requirements.

Centralized Storage and Backup Operations

- Centralized storage (typically H:, I:, Y:, Z: drives) should be the primary storage area for all users and must be the primary storage for administrative users and administrative data as well as for any data that is categorized as restricted or confidential. Routine backups are made of centralized storage on a scheduled basis.
- To facilitate rapid recovery of data should it be accidentally deleted or there is a failure of central storage, academic users may wish to keep local or off-line copies of files that do not contain confidential or restricted data.
- May not store or make available copyrighted or protected content or software without proof of authorization to do so.

Access, Authorization, and Authentication Requirements

- Multi-factor authentication should be required where appropriate (such as for physical access, admin access, etc.) and possible.
- Role-based authorization should be implemented where appropriate.
- Single sign-on and federated identity technologies should be used where possible to minimize the proliferation of multiple credentials.
- Passwords and passphrases must meet minimum criteria for length and complexity (based on system type).
- Passwords must be changed on a periodic basis as dictated by system/application or other requirements.

Access to, and Protection of, Institutional Data (as described in document ***"Data Classification and Roles Definitions"*****)**

- Access to institutional systems and/or data must be authorized by the appropriate administrative official.
- You are expected to understand the classification and sensitivity level of data you access. (Classifications are described in the document ***"Data Classification and Roles Definitions".*****)**
- You may only access data needed to carry out your responsibilities as an employee or a student.
- You must protect the integrity and confidentiality of institutional data regardless of the form or location of data.
- You must shred, destroy, or otherwise render unusable any physical document or storage device that is to be discarded that contains or has contained confidential or restricted data.
- Institutional data that is stored on any laptop, portable device, or portable storage media must be encrypted.

Cloud-based Applications and/or Contracted Services

- Potential cloud-based application or service offerings must undergo a thorough security review by appropriate CCIT staff and receive approval of the CIO prior to being selected or any contract being signed.

Compliance with Federal, State, Local Law and Institutional Policies

- You are expected to be aware of, and comply with, all IT-related federal, state, and local laws as well as CSM policies. Of particular note are the following:
    - Digital Millennium Copyright Act (1998)
        - *Updated US copyright law enacted in 1998 for the digital age.*
    - Family Educational Rights and Privacy Act (FERPA, 1974)
        - *Protects the privacy of student educational records and provides for the opportunity to amend records.*
    - Health Insurance Portability and Accountability Act (HIPAA, 1996)
        - *Protects health insurance coverage for workers when they change/lose jobs, protects the privacy of health records, and requires national standards be established for electronic health care transactions.*
    - Federal Trade Commission "Red Flags Rule" (2008)
        - *Defines how certain organizations must develop, implement, and administer identity theft prevention and notification programs.*
    - Computer Fraud and Abuse Act (CFAA, 1986)
        - *Enacted in 1986 as an amendment to existing computer fraud law. Amended several times to keep up with changing technology and circumstances.*
    - Electronic Communications Privacy Act (ECPA, 1986)
        - *Places restrictions on "wiretapping" of transmissions of electronic data by computer similar to those of telephone calls. Amended by the Communications Assistance for Law Enforcement Act (CALEA) in 1994, the USA PATRIOT Act (2001 and 2006), and the Foreign Intelligence Surveillance Act (FISA) Amendments Act (2008).*
    - Technology, Education, and Copyright Harmonization Act (TEACH, 2002)
        - *Establishes and clarifies compliance measures institutions are required to use to protect copyrighted material in distance education environments.*

General

- You are expected to report suspect activities.
- Beware of phishing attempts – many are well crafted. Mines support staff will never ask for your password in an email.