1.0 BACKGROUND AND PURPOSE

The Colorado School of Mines (“Mines”) is committed to providing the tools necessary to conduct university business. As part of this commitment, Mines provides electronic mail services to support the academic, research, and administrative functions of the university. The Policy and Procedures below set forth the requirements governing the use of E-mail services and Mines E-mail accounts.

It is the intent of this Policy to meet the guidelines laid out in NIST SP 800-45.

2.0 POLICY STATEMENTS

All official university business and communications must be conducted using Mines E-mail accounts.

Subscriptions to Mines related distribution groups or lists require members to use their official Mines E-mail address for communications unless the list is specifically targeted to members outside the Mines E-mail organization such as Mines alumni or other former Mines students, or employees.

All E-mail communications and associated attachments transmitted or received over the Mines network are subject to the provisions of this Policy and the Procedures in Exhibit I.

Subject to State and Federal laws, rules and regulations, and university policies, all information created, modified and/or stored on university computing equipment is the property of Mines. This includes Mines’ employee E-mail accounts, E-mail communications conducted with such accounts, and all information stored on any computer or network device owned by Mines or procured with university funds. There is no expectation of privacy for business E-mail messages sent through or to university E-mail accounts (MyMail and/or Office365).

Use of a personal E-mail account (e.g., Gmail, Hotmail, Yahoo or any similar external/third-party E-mail services) to conduct university business is prohibited.
Automatic forwarding or redirecting of messages to a non-Mines address using inbox rules or other automated mechanism is not permitted. Any inbox rule with forwarding or redirect rules pointing to an address outside the organization may be removed without warning. Forwarding to another Mines address, or Mines maintained server, may be permitted on a limited basis depending on the circumstances and need of such forwarding.

3.0 RESPONSIBILITIES

The university provides an official university E-mail account to all employees (full-time, part-time, temporary, and student employees), students, appropriate affiliate staff, and certain authorized third-parties for conducting university business. All users of Mines E-mail services are responsible for using the services in an efficient and professional manner, consistent with university Policies, Procedures, and applicable laws.

Individuals with special relationships with Mines, such as alumni or affiliates, who are neither employed nor enrolled at Mines, are granted limited E-mail privileges, including an E-mail address commensurate with the nature of their special relationship (See additional information in Section 2.5 of the attached Procedures). These accounts are subject to the provisions of this Policy and Mines reserves the right to discontinue these privileges at any time.

3.1 Security. Mines uses reasonable and prudent efforts to provide secure and reliable E-mail services consistent with established information technology practices. However, Mines cannot guarantee the security, privacy, or reliability of its E-mail service. All E-mail users, should exercise caution in using their Mines E-mail accounts to communicate confidential or sensitive matters and prevent the spread of viruses.

Insecure devices should not be used to access E-mail that may contain Confidential or Personal Data (each as defined in the Administrative Data Policy). Secure devices are PIN or password protected, include anti-malware software, and use a modern, supported operating system.

3.2 Privacy. E-mail messages can be intercepted, stored, read, modified, and/or forwarded to other recipients, therefore additional care must be exercised anytime sensitive information is exchanged via E-mail. Highly Confidential Data (e.g., social security numbers, credit card numbers, financial account numbers, and similar data) should never be included in E-mail. Confidential or Personal Data should be transferred through a secure and encrypted portal, regardless of whether the transmission is made to individuals within or outside of the campus environment.
Confidential Data should be communicated using a @mines.edu address. Any communication using an address that is not @mines.edu is considered external and must be encrypted using Secure/Multipurpose Internet Mail Extensions (RFC 8551).

Users who need to exchange encrypted E-mail with individuals outside the campus environment should contact Information and Technology Solutions (ITS) for assistance setting up the required features.

Individuals communicating Confidential Data outside of the university are strongly encouraged to avoid email altogether and make use of the university’s secure file exchange tool known as Blasters Pannier.

3.3 SPAM & Phishing. All incoming E-mail is scanned for viruses, Phishing attacks, and SPAM. Suspected messages are blocked from the user’s inbox.

In many cases, viruses or Phishing appear to be sent from a friend, coworker, or other legitimate source. E-mail users should not click links or open attachments unless the user is sure of the nature of the message. If any doubt exists, the E-mail user should submit a ticket to the Mines Service Center by selecting the category: Email/Calendar and service: Phishing Issue.

SPAM messages can be forwarded to spam@mines.edu. Suspected phishing emails can be forwarded to phishing@mines.edu.

4.0 COMPLIANCE/ENFORCEMENT

The university may suspend or revoke the E-mail privileges of any user who does not comply with this Policy and Procedures. Mines may take necessary corrective action, ranging from reprimand to termination, upon a user who violates this Policy and Procedures.

Mines reserves the right to temporarily disable or suspend any account that may pose a security risk to Mines network or data as determined by ITS. If the risk cannot be reasonably mitigated, Mines reserves the right to permanently delete any account that may pose a risk to Mines network or data.

5.0 DEFINITIONS

Conditional Access Policies means a function in which a user’s access to E-mail (also relevant applications, documents and information) is managed by setting conditions on the access to this data so the organization has more control over who accesses the data and where and in what way the information is accessed.

Conditions could include:
• Geographical location
• IP address and network
• Used device
• Browser
• Operating System (OS)

**E-Mail** means an electronic message transmitted between two or more computers or electronic terminals, whether or not the message is converted to hard copy format after receipt and whether or not the message is viewed upon transmission or stored for later retrieval. E-mail includes electronic messages that are transmitted through a local, regional, or global computer network.

**Phishing** means the attempt to acquire sensitive information such as usernames, passwords, and credit card details (and sometimes, indirectly, money), often for malicious reasons, by masquerading as a trustworthy entity in an electronic communication.

**SPAM** means unsolicited and undesired advertisements for products or services sent to a large distribution of users.

### 6.0 RESOURCES or ATTACHMENTS

- NIST SP 800-45
- ITS Website
- Administrative Data Policy
- Employment Communications Policy
- Colorado Open Records Act, §24-72-201, *et seq.*

### KEY WORDS

E-mail, Spam, Phishing, forwarding, POP3, IMAP, security, privacy, account, exchange, google, office365, mymail.

### 7.0 HISTORY AND REVIEW CYCLE

The Policy will be reviewed at least annually, or as needed by the Responsible Administrative Unit.

Updated/Amended March 10, 2021 (changed formatting and layout; updated terminology phrasing, technologies, and procedures)
Electronic Mail Policy

EXHIBIT 1 - PROCEDURES

1.0 PROCEDURES PURPOSE

These Procedures set forth the guidelines for the responsible and efficient use of E-mail services and appropriate use of official university E-mail accounts.

2.0 PROCEDURES

2.1 Prohibited E-Mail Practices. Users of Mines E-mail services are prohibited from engaging in any of the following practices on the Mines network:

- a) Sending obscene or patently offensive E-mail without the consent of the recipient;
- b) Sending intimidating, threatening, harassing, or abusive E-mail;
- c) Intercepting, disrupting, or altering an E-mail communication without proper authorization;
- d) Accessing, copying, or modifying E-mail messages from or within the electronic files or records of another without permission;
- e) Misrepresenting the identity of the source of an E-mail communication;
- f) Allowing another individual to use one's E-mail account for fraudulent purposes;
- g) Using E-mail to interfere with the ability of others to conduct Mines business;
- h) Sending unsolicited "junk" E-mail or mass electronic mailings, such as chain letters, without a legitimate Mines business purpose;
- i) Using E-mail for commercial purposes unrelated to Mines business;
- j) Reproducing or distributing copyrighted materials without appropriate authorization; and
- k) Using E-mail for any purpose in contradiction to state law, federal law, or Mines policy.

2.2. University Monitoring and Disclosure. Under certain circumstances it may be necessary for ITS staff or other university officials to access university E-mail accounts. These circumstances may include, but are not limited to, maintaining the system, investigating security or abuse situations, internal investigations, or responding to a legal request, including but not limited to a legal hold, discovery request, subpoena, or court order. ITS or other university officials may also require access to a Mines E-mail account to continue business where the university account holder will not or can no longer access the account for any reason, including but not limited to, disability, illness, death, or separation from the university temporarily or permanently. Such access will be granted on an as-needed basis.
Mines reserves the right to monitor E-mail usage of employees from time to time and without prior notice. Such monitoring may include tracking addresses of E-mail sent and received, accessing in-box messages, accessing messages in folders, and accessing archived messages. E-mail monitoring which focuses on a specific individual or a selected group of individuals must be based on a reasonable suspicion of misuse or wrongdoing and must be approved in advance by the appropriate Vice President or the President. Mines may take corrective action or disciplinary action against an employee based upon information obtained from monitoring or inspecting his or her E-mail communications.

Mines reserves the right to disclose the contents of university E-mail accounts without the consent of the user. The university will do so when it believes it has a legitimate business need and when authorized by the appropriate university authority or applicable law. Contents may be disclosed to those individuals having a reasonable business purpose, or as necessary to protect health and safety of university or community members, to assist law enforcement, or to comply with legal requirements. Furthermore, Mines may disclose E-mail communications sent to, received by, or relating to an employee to law enforcement officials without giving prior notice to the employee.

In limited situations, E-mail related to a student may constitute an "education record" subject to the provisions of the Family Educational Rights and Privacy Act of 1974 (FERPA) 20 U.S.C. §1232g; 34 CFR Part 99. Under such circumstances, the university may access, inspect, and disclose such records as permitted by FERPA and consistent with Mines’ annual FERPA notice.

2.3 Application of Public Records Statutes to E-Mail. E-mail messages are subject to legal requirements governing public records of State institutions of higher education, including the Colorado Open Records Act, §24-72-201, et seq., C.R.S. (1997), as amended ("CORA"), which governs public access to Mines records, and the Archives and Public Records Act, § 24-80-101, et seq., C.R.S. (1997), as amended, which governs the retention, archiving, and destruction of Mines documents and records.

Under CORA, writings, whether in paper or electronic form, made, maintained, or kept by Mines are generally considered to be public records and are subject to public inspection unless they are covered by a specific statutory exception. Correspondence of Mines’ employees in the form of E-mail may be a public record subject to public inspection under section § 24-72-203 C.R.S. of CORA.

The Archives and Public Records Act requires that all documents pertaining to the business of Mines, whether in paper or electronic form, be retained, archived, or destroyed, as appropriate. E-mail messages that are public records must be retained in either paper or electronic format. E-mail messages that are not public records should be deleted after viewing.
2.4 E-mail Disposal and Retention. An E-mail box is not an appropriate place to retain university records; records that are in a user’s E-mail should be removed to other proper storage media intended for archival purposes.

2.5 Expiration of Accounts. Individuals may leave the university for a variety of reasons, which gives rise to differing situations regarding the length of E-mail privileges or expiration of accounts. The guidelines governing those privileges are set forth below.

- Faculty who leave before retirement – Faculty who leave before retirement will have E-mail privileges removed effective on their last worked day. If such separation is for cause, E-mail privileges may be immediately revoked without notice.
- Staff who leave before retirement – Staff members who leave the university will have E-mail privileges removed effective on their last worked day. If such separation is for cause, E-mail privileges may be immediately revoked without notice.
- Emeritus Faculty – Faculty who have retired from the university and have Emeritus status will be permitted to retain their E-mail privileges if their account remains active. All E-mail accounts that are inactive for a period of one year will be removed.
- Retired Staff – Staff who have retired from the university will have E-mail privileges removed effective on their last worked day.
- Students who leave before graduation – Students who leave the university without completion of their degree or other program may keep their E-mail privileges until the end the last term when they were registered.
- Expelled students – If a student is expelled from the university, E-mail privileges will be terminated immediately upon the directive of the Dean of Students Office.
- Alumni – Students who have graduated with a degree from the university will be permitted to retain E-mail privileges if their account remains active. All E-mail accounts that are inactive for a period of one year will be removed. Alumni wishing to reconnect with the university can request an Alumni account and one may be provided to them. In the event the university terminates or otherwise ceases its contractual relationship with Google and/or Microsoft, those with Alumni accounts may lose E-mail and other privileges for those accounts in accordance with the terms of the Google and/or Microsoft contract. Notice will be provided as soon as reasonably possible.
- Deceased faculty, staff, or student – Upon receiving notice of the expiry of a student, faculty, or staff from the university, the following procedures will be used:
  a) E-mail privileges will be terminated immediately upon the directive of the Office of General Counsel, Dean of Students, and/or Human Resources.
b) **Employees.** The department may exercise discretion in determining how to handle the deceased employee’s business email account including whether to have the deceased person’s E-mail automatically forwarded to another account if they received departmental requests or a considerable volume of business correspondence. In addition, an automatic reply message may be returned to senders. ITS makes these changes on the department’s behalf.

Based on the amount and type of email received by the decedent, ITS may set up an auto-reply with no forwarding: An automatic reply will be sent to the original sender, “The account for jane-doe@mines.edu has been closed. If you need assistance please resend your message to mary-smith@mines.edu.”

c) **Students.** FERPA protection of personally identifiable information in a student’s education record ends at the time of a student’s death. Mines’ policy on the release of a deceased student’s records is as follows:

Within the first year following the death of a student, the university will release the educational records of the decedent to the following individuals:

- If the student submitted a signed Authorization to Release Educational Records form which designated the person(s) eligible to request and/or receive educational records, the information will be released to the individual on that form.
- The decedent’s next of kin, provided that the request is accompanied by official documentation.
- The individual designated as the personal representative of the decedent’s estate, provided that the request is accompanied by official documentation.
- Members of the family or other persons with the written approval from the decedent’s next of kin or the personal representative of the decedent’s estate. Absent written approval from the family or representative of the estate, only directory information will be disclosed.
- In response to a subpoena or court order.
- To any other individual, if determined by the university to be in the best interest of the decedent or the university.

After one year has elapsed following the death of an individual student, the university may release the educational records of the decedent at the university’s discretion.

2.6 **Use of POP, IMAP & Modern Authentication.** In order to comply with the modern methods of authentication, Mines will disable the ability for all users to
Electronic Mail Policy

have POP enabled for their mailbox, with only few exceptions for service mailboxes or other shared mailboxes with specific needs.

- Post Office Protocol (POP) connections will not be supported.
- Internet Message Access Protocol (IMAP) connections will be supported but must use OAUTH for authentication. "Password" or “Basic” authentication is not supported for user mailboxes using the IMAP protocol.

All mail clients must use Modern Authentication Methods in order to access E-mail. Specific E-mail clients (e.g., Microsoft Outlook, Apple Mail, Thunderbird, and others) may vary over time but should support Modern Authentication Methods and be fully supported by the specific vendor. Mail readers that do not support Modern Authentication Methods are not allowed by Mines. Mail clients used to access Mines E-mail must be vendor supported with timely security patches issued.