COLORADO SCHOOL OF MINES	**Administrative Data Policy**	**Responsible Administrative Unit:** Information & Technology Solutions
	Issued: March 2014 **Revised: September 2019**	**Policy Contact:** Chief Information Officer msendze@mines.edu

1.0 BACKGROUND AND PURPOSE

The Colorado School of Mines' ("Mines", "the School", or "the Institution") administrative data must be managed and protected because it is a critical and valuable asset to the school and its mission. The purpose of this policy and related policies and procedures is to protect the school's administrative data from accidental or intentional unauthorized access, damage, alteration or disclosure, while also preserving the ability of authorized users to access and use administrative data for appropriate purposes.

2.0 SCOPE

Administrative data covered by this policy include all of the following regardless of the format of the data or where or how it is housed:

2.1 All data created, collected, maintained, recorded or managed by the institution, its staff, and agents working on its behalf.

2.2 All data used for planning, managing, operating, controlling, or auditing institutional functions; especially data used by multiple units of the school; and data used for institutional reporting.

2.3 All operational data regardless of its source (e.g. extracts or feeds from or to the institution's enterprise systems; shadow systems whether independently created by institutional units or assembled from enterprise systems extracts or both.)

2.4 All data which contains *Personal Data*.

2.5 All data that contains proprietary information and/or trade secrets.

This policy applies to all members of the Mines community whether students, faculty, staff, or their agents, and all divisions, departments and other units, their agents, and their contractors. To the extent possible, this policy applies to any person or entity in possession of administrative data whether affiliated with Mines or not.

3.0 POLICY

All members of the Colorado School of Mines community who work with or use administrative data in any manner must comply with all federal, state, and privacy laws, and other applicable school policies, procedures, industry standards, contracts and licenses (e.g., FERPA, HIPAA, GLBA, HIGHTEC, PCI, etc.). School employees and their supervisors are responsible for ascertaining, understanding, and complying with all laws, rules, policies, standards, contracts and licenses which apply to their own and their subordinates' specific uses of administrative data.

4.0 OWNERSHIP, ACCESS AND USER RESPONSIBILITIES

Access and use of administrative data is governed by data type. Many positions on campus have specific responsibilities based on their functional role for handling data, also defined in the "Data Classifications and Roles Definitions" document. All data must be treated with care/respect regardless of its defined type. Please adhere to the Data Code of Conduct for guiding principles for using data.

4.1 Access

4.1.1 Access to all data is granted solely to fulfill the legitimate business need(s) documented for a position. The principle of least privilege should be used to provide the user with the minimum permissions they need to perform their work.

4.1.2 Access to all data must be approved by both the individual's department head and the System Owner.

4.2 Collection

4.2.1 *Personal Data* should not be collected if not required for the business function.

4.3 Use

4.3.1 All data are used by authorized individuals only as required to conduct the legitimate business of the School as assigned to their position. All data may not be collected, accessed, used, disclosed, modified, or deleted for personal gain or curiosity or for another's personal gain or curiosity.

4.3.2 All data may not be shared with other School employees or anyone else, unless those persons have authorization to view the data to conduct the legitimate Business of the School.

4.3.3 All data may only be released or disclosed outside of the Institution by an authorized *Certifying Authority*.

4.4 Storing

4.4.1 *Public Data* – Data on web sites intended for the general public do not require authorization by a data steward or *Certifying Authority* as long as their content does not imply an official statement or position of the school.

4.4.2 *Restricted* and *Confidential Data* (including *Personal Data*) –

Where possible, data should not be stored or copied to local devices on desktops or mobile devices such as smartphones, laptops or USB keys. In rare circumstances where that is not practical, the stored data must be encrypted. Although it is recognized that exceptions to this do exist, any data stored on mobile devices must be encrypted according to the Executive Directive titled "*Mandatory Use of Encryption Software for Mobile Devices*".

Paper copies are to be kept in locked filing cabinets in physically secure areas that are accessible only by authorized individuals. Keep the number of copies to a minimum.

4.5 Disclosure

4.5.1 *Restricted Data* – Users and Data custodians are authorized to disclose these data as directed by data stewards

4.5.2 *Confidential Data* – Only the Data Steward is authorized to disclose these data

4.5.2.1 *Personal Data*

Disclosure of *Personal Data* outside of Mines must be reviewed by the Privacy Compliance Director.

Unless Mines' retains the primary responsibility for implementing and maintaining reasonable security procedures and practices, third party service providers, to which Mines' discloses *Personal Data*, must implement and maintain reasonable security procedures and practices that are:

- Appropriate to the nature of the *Personal Data*; and
- Reasonably designed to help protect the *Personal Data* from unauthorized access, use, modification, disclosure, or destruction. [C.R.S. 24-73-102]

- Consent should be collected from the individual prior to disclosure when required by applicable state or federal laws or regulations. [C.R.S. 24-90-119] [GDPR]

4.6 Retention

4.6.1 *Personal Data*

When *Personal Data* is no longer needed, it should be destroyed in accordance with state or federal law or regulation. Any document containing *Personal Data* must be securely disposed of by shredding, erasing, or otherwise modifying the *Personal Data* to make it unreadable or indecipherable through any means. [C.R.S. 24-73-101]

Personal Data (whether paper or electronic) cannot be disposed of, even after the retention period has passed, when there is a formal request pending for that data (e.g., subpoenas or Colorado Open Records, etc.).

Third-parties or vendors should provide assurance or supporting documentation with retention and secure destruction practices of Mines' *Personal Data*.

5.0 SYSTEM AND SECURITY CONSIDERATIONS

Computers and other devices used with administrative data must comply with all requirements detailed in the Security Practices and Guidelines document for the classification of data being used with the device. Furthermore, systems, processes, procedures, storage facilities, etc., using a collection of administrative data which fall within more than one data classification, must protect the entire collection according to the collections' data with the highest classification.

6.0 VIOLATIONS

Suspected or actual breaches, losses or other inadvertent or unauthorized exposure of administrative data (regardless of its data classification), must be immediately reported to the Chief Information Security Officer (CISO). If *Personal Data* is involved, it must also be reported to the Privacy Compliance Director. If actual or suspected criminal or fraudulent activity may also be associated with an administrative data event, appropriate law enforcement must be advised as well. Alleged violations of the IT policy and/or procedures 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 materials.

7.0 DEFINITIONS

Certifying Authority – see Data Classification and Roles Definitions

Confidential Data – see Data Classification and Roles Definitions

Personal Data – see Data Classification and Roles Definitions

Public Data – see Data Classification and Roles Definitions

Restricted Data – see Data Classification and Roles Definitions

8.0 RESOURCES or ATTACHMENTS

- Data Code of Conduct
- Data Classification and Roles Definition
- FERPA-protected Data Policy
- GDPR Notice