| | | |
|---|---|---|
| COLORADO SCHOOL OF MINES | **Administrative Data Policy** | |
| | **Responsible Administrative Unit:** Information & Technology Solutions | **Policy Contact:** Chief Information Officer, ocio@mines.edu |

## 1.0 BACKGROUND AND PURPOSE

The Colorado School of Mines ("Mines") is committed to ensuring the integrity of Administrate Data, including but not limited to, accuracy, security, management, appropriate access and use. Administrative Data plays a valuable role in Mines achieving its mission and is a critical factor in decision-making.

As part of this commitment, Mines has promulgated this Policy and associated Procedures to set forth the requirements for data governance (including roles and responsibilities, protecting administrative data, and ownership of data.

## 2.0 POLICY STATEMENT(S)

Mines own all Administrative Data. See Exhibit 1 – Procedures, Section 2.1 for examples of data covered under this policy. Access to and use of Administrative Data must be limited to Mines business needs.

Use of Administrative Data is subject to terms of use, as outlined in the IT Appropriate Use Policy, or use as otherwise approved by the Data Trustee Board.

Administrative Data must be consistently protected throughout its lifecycle in a manner commensurate with its classification regardless of the Data Repository used, the form it takes, the technology or methods used to manage it or the purpose it serves. The classification system for Administrative Data is included in Exhibit 1 – Procedures Section 2.3.

Computers, systems, processes, procedures, Data Repository, etc., using Administrative Data covering more than one data classification category, must protect the entire collection according to the highest (i.e., most protective) data classification category. Data protection procedures must comply with all requirements detailed in the Required ITS Security Practices and Guidelines.

## 3.0 RESPONSIBLITIES

All members of the Mines community and Affiliates are responsible for using and protecting Administrative Data and complying with all applicable Mines policies and

procedures, as well as, international, federal and state laws. There are specific roles defined for individuals using/protecting Administrative Data:

The Mines Chief Data Officer ("CDO") is responsible for leading and coordinating all activities related to Administrative Data management. The CDO will ensuring that each functional area develops and implements processes for identifying and correcting erroneous or inconsistent data. The CDO will develop training related to this Policy and administer the training to the various data roles.

Data Users are individuals who access Administrative Data to perform their assigned duties. Data Users are responsible for their own appropriate use and interpretation of the data they access according to the Mines Appropriate Use Policy.

The Data Trustees, as a group, have oversight responsibility for Administrative Data related to the functions managed, administered or run by the units and personnel who report to them. Each Data Trustee must be responsible for developing a plan for their Business Domain (as defined in Appendix A) to assess the risk of erroneous or inconsistent data and, if found, indicate how such erroneous or inconsistent data will be corrected.

Data Stewards are assigned by a Data Trustee and have the primary responsibility for the classification, accuracy, privacy, security and retention of their Business Domain data subsets.

ITS Data Custodians are assigned to each Source Data Systems which maintains Administrative Data. The ITS Data Custodians oversee the safe transport and storage of data, establish and maintain the underlying infrastructure, and perform activities required to keep the data intact and available to users.

The Institutional Research and Strategic Analytics (IRSA) Department is responsible for working with the appropriate Data Stewards to develop definitions of commonly used terms, provide guidance on state and federal data definitions, and will define how official Mines metrics are calculated.

Additional information about specific roles related to Administrative Data is included in Exhibit 1 – Procedures, Section 2.2.

## 4.0 COMPLIANCE/ENFORCEMENT

Suspected or actual breaches, losses or other inadvertent or unauthorized exposure of Administrative Data (regardless of its classification), must be immediately reported to the Chief Information Security Officer (CISO). Administrative Data events that involve personal data must be reported to the Compliance Office. If actual or suspected criminal or fraudulent activity is associated with an Administrative Data event, the Chief Information Officer (CIO) or CISO will advise appropriate law enforcement.

Notification of breaches, losses or other inadvertent or unauthorized exposure will follow all ITS security or privacy compliance incident notification procedures, as applicable.

Failure to comply with the Administrative Data Policy and Procedures may result in sanctions relating to the individual's use of information technology resources (such as suspension or termination of access, or removal of online material); the individual's employment (up to and including immediate termination of employment in accordance with applicable university policy); the individual's studies within the university (such as student discipline in accordance with applicable university policy); civil or criminal liability; or any combination of these.

## 5.0 EXCLUSIONS

Research data used to conduct investigations and validate research findings in the scientific community is excluded from this policy. However, research Administrative Data such as proposals, awards, compliance records, patent and invention Information is included.

## 6.0 DEFINITIONS

**Administrative Data** means data that is collected to support Mines administrative operations, including but not limited, to the following Business Domains; institutional administration, research administration, student administration, student life administration, employee information, faculty information, financial resources, budget resources, academic affairs, campus resources, services and facilities.

**Affiliate(s)** means organizations that are connected or affiliated to Mines, often as a branch or subsidiary part of Mines; that is associated with a main or major group within Mines; or are an affiliate or member. Examples could include Sodexo, Barnes and Noble Bookstore, Mines Foundation.

**Data Access and Use Agreement** means external agreements that clearly document what Administrative data are being shared between Business Domains and Affiliates and how the data can be used.

**Data Repository** means any Mines controlled storage infrastructure whether on premise, hosted, or with a cloud provider. Examples include One Drive, Network Shared Drive, Survey Management Systems, Marketing & Communications Systems, alternate data centers, and other systems.

**Data Sharing Agreements** means internal agreements that clearly document what Administrative data are being shared and how they can be used.

**Source Data Systems** means systems that aid in the collection of Mines Administrative Data for effective and efficient operations, including but not limited to Enterprise Resource Planning (ERP), Operations Data Store (ODS), Enterprise Data Warehouse (EDW), Customer Relationship Management (CRM), Applicant Tracking Systems, and other systems.

## 7.0 RESOURCES

- **Data Code of Conduct**
- **Required IT Security Practices and Guidelines**
- **IT Appropriate Use Policy**
- **Records Retention Policy**
- **Student Data Access Policy**
- **Family Educational Rights and Privacy Act (FERPA) Policy**
- **Privacy Statement**
- **Export Controls**
- **ITS Policy Violations Processes**

## 8.0 HISTORY AND REVIEW CYCLE

The policy will be reviewed at least every 2 years, or as needed by the Responsible Administrative Unit.

Issued: March 2014
Updated: September 2019
Updated: June 23, 2021 (combined with Data Classification and Roles Definitions, changed formatting and layout, updated terminology, additional guidance added)

## EXHIBIT 1 - PROCEDURES

### 1.0 PROCEDURES PURPOSE

In order for Mines to effectively manage and protect Administrative Data; Procedures must be in place to guide appropriate access to Administrative Data, ensure the security of Administrative Data and provide a data governance structure with well-defined roles and responsibilities. These Procedures apply to any person or entity (whether affiliated with Mines or not) in possession of Administrative Data, regardless of means of use, storage or extraction from any Data Repository.

### 2.0 PROCEDURES

**2.1 Administrative Data Examples.** Examples of the type of data covered by this Policy and Procedures, include but are not limited to, Mines data:

- created, collected, maintained, recorded or managed by Mines, its staff, and Affiliates working on Mines behalf;
- used for planning, managing, operating, controlling, or auditing institutional functions;
- used by multiple Mines units;
- used for institutional reporting;
- containing personal data;
- containing proprietary information and/or trade secrets; and
- designated as Controlled Unclassified Information (CUI) by the US Government.

**2.2 Roles for Handling Administrative Data.** Defined roles and data management responsibilities should be included in employees job descriptions to help ensure approved protocols for data management are maintained.

**A.** Data Trustees (e.g., Controller, Vice Provost Enrollment Management, AVP Student Life, COO, and Executive Director of Financial Planning)

- Provide oversight and ensure appropriate access for the protection, integrity and usefulness of Administrative Data within their Business Domain.
- Ensure their employees are in compliance with external regulations and internal policies.
- Establish the appropriate levels of training for individuals given access to Administrative Data within their Business Domain.
- Coordinate with the CISO and Compliance Office regarding training on data security and use of personal data.
- Assign one or more Data Stewards to be responsible for data management of their Business Domain.

- Establish appropriate security restrictions for sharing Administrative Data between Mines academic and/or administrative.
- Participate as an active member of the Data Trustee Board.

**B.** Data Stewards (e.g., Registrar/Associate Registrar, Executive/Associate Director of Admissions, Director/Associate Director of Financial Aid, Director/Associate of Human Resources, Director/Associate Director of Business Systems, Dean of Students, Director/Associate Director of Athletics, Budget Director, Director of Academic Affairs Operations, Director of Maps, Bursar, Director of Research Administration, Director of Title IX, Associate Dean, Director of Maps, Bursar, Academic Affairs Operations Manager and Federal Contracts Administrator)

- Participate as an active member of the Data Stewardship Working Group.
- Implement controls to ensure the integrity, security, and privacy of the data.
- Work with all data roles to quickly resolve data issues and develop automated processes to identify erroneous, inconsistent, or missing data.
- Support and implement Mines policies in collaboration with CDO and other data stewardship roles.
- Maintain and facilitate Data Access and Use Agreement between Business Domains and Affiliates.

**C.** ITS Data Custodian (e.g., Enterprise Solutions, Business Systems, and Institutional Research and Strategic Analytics teams)

- Have modification or distribution privileges. Must coordinate distribution/disclosure of data with Compliance Office to ensure privacy compliance.
- Protect data and prevent unauthorized use.
- Maintain and report user access to systems they manage.
- Maintain and facilitate Internal Data Sharing Agreements.
- Support Mines policies in collaboration with Data Stewards.
- In conjunction with Data Stewards and the CDO, develop automated processes to identify erroneous, inconsistent, or missing data.

**D.** Data User (e.g., President, CFO, COO, Academic Affairs Provosts and Vice Provosts, Dean of Graduate Studies, Dean of Undergraduate Studies, administrative assistants to Academic Deans and Academic Departments, DHDDs, ADHDDs)

- Safeguard their individual access privileges.
- Adhere to all applicable Mines policies.
- Secure and protect data and data privacy.

**E.** Institutional Research and Strategic Analytics (IRSA) Department

- Report data discrepancies and inconsistencies to the appropriate Data Steward for resolution.
- Perform data analysis and report generation for customers that include external agencies (federal and state), external data requestors, and all Business Domains.
- Coordinate with CISO and Compliance Office prior to sending data to external agencies/data requestors.

**F.** Data Trustee Board (composed of the Data Trustees; chaired by the CDO)

- Establish overall policies for management and access to the Administrative Data.
- Review and approve all procedures developed in each Business Domain area by the Data Stewards to ensure appropriate compliance with this Policy.
- Provide oversight of all processes that capture, maintain and report on Administrative Data.
- Approve the retention and archiving of Administrative Data.

**G.** Data Stewardship Working Group (composed of the Data Stewards, ITS Data Custodians; chaired by CDO; other designated data roles may be invited to participate, as appropriate)

- Review the operational effectiveness of Administrative Data management policies and procedures and make recommendations to the Data Trustee Board for improvement or change.
- Share best practices and raises concerns across Business Domain areas.
- Ensure regular and appropriate collaborative communication with Data Users on any operational changes that effect business processes and data.

**2.3 Data Classification.** Administrative Data is classified according to its criticality, confidentiality, and the risk of harm that would be caused by unauthorized, inadvertent, or deliberate disclosure, alteration, or destruction. The Administrative Data classifications below are listed in increasing risk of impact of mishandled data:

**A.** Public: No access restrictions and are available to the general public.

- High level enrollment statistics
- The Undergraduate and Graduate Bulletins
- All Funds Budget
- Financial statements
- Press releases
- Posted advertisements
- Newsletters

- Some research data

**B.** Restricted: Typically not protected by law or regulation, but must be guarded due to proprietary, ethical, or general privacy considerations, and for which unauthorized disclosure, alteration, or destruction would cause perceivable damage to the school. Unless formally classified otherwise, all Mines data is classified as restricted.

- Newsletters
- Some purchasing data
- Information covered by non-disclosure agreements
- Operational procedures which are either proprietary to Mines or which could jeopardize personal or public safety if disclosed
- Some research data

**C.** Confidential: Any data which would cause significant damage to Mines or to one of its constituents if breached, disclosed, modified or destroyed without specific authorization. Unless otherwise specified in another policy, the highest level of security and controls must be applied to protect confidential data.

1. Statutorily or contractually protected data. All data that is protected by state or federal laws, regulations, or rules and data covered under a Mines contractual or licensing agreement.

    - Education records as governed by the Mines' FERPA policy
    - Individuals' financial aid data and tax data
    - Library user records: any record or other information that identifies a person as having requested or obtained specific materials or service or as otherwise having used the library
    - Usernames and password combinations
    - Social security numbers
    - Credit card and financial institution account numbers and other personally identifiable information
    - Sensitive information; information about a person including religious or philosophical beliefs, race, ethnicity, political opinions or trade union membership, sexual life & orientation, genetic or biometric information, health information, and criminal convictions
    - Data collected during times of emergency and routine internal procedures to protect the public health and welfare
    - Some research data
    - Classified and Export Control

2. Personal data. Non-public information that can identify a person, directly or indirectly, by an identifier. Personal data must only be used for the purpose

for which it was collected. Directly identifiable data includes, but is not limited to: name, address, personal identifier such as social security number, campus-wide ID, biometric record, official state or government issued license or ID card, passport number, photo or video, phone number, and credit card information. Indirectly identifiable data includes, but is not limited to: date of birth, birthplace, mother's maiden name, location data, online identifiers, as well as combinations of data.

- One or more physical, physiological, genetic, mental, economic, cultural, or social identifier
- Username or email plus password or security questions/answers
- Gender, zip code, and date of birth

3. Controlled Unclassified Information (CUI). Identified by the US Government. This data must be protected according to US Government security standards outlined in the Defense Federal Acquisition Regulations (DFARS) and National Institute of Standards document (NIST-SP 800-171b)

    - All Title IV data

**2.4 Data Access.** Employees require access to the Administrative Data needed to perform their responsibilities. Access to Personal data should be limited to individuals with a business need, but should exclude all others. The CDO is responsible for ensuring that procedures are developed by Business Domains to address those cases where a member of Mines community seeks permission to access Administrative Data beyond the normal performance of their duties. The appropriate campus officials must be consulted for issues related to personal data, legal concerns or other areas.

Before an employee is permitted access to Administrative Data in any form, training in the use and attributes of the data, functional area data policies and applicable Mines policies is required.

**2.5 Data Management.** Wherever possible, a uniform set of definitions for commonly consumed Administrative Data should be used throughout Mines (e.g., "enrolled student" should have the same meaning across all departments).

Administrative Data should be integrated into Source Data Systems to reduce duplication of data collection and foster data accuracy across the various data systems.

**2.6 Disclosure of Administrative Data.**

**A.** Data Users must consult with Data Trustees or Data Stewards of the respective Business Domain prior to releasing any Administrative Data.

**B.** The Office of Legal Services must coordinate all responses to third-party requests for Administrative Data made through subpoenas or Colorado Open Records (CORA) requests.

**C.** Institutional Research and Strategic Analytics must be consulted for university-wide studies and use of any and all aggregate data that is requested by all non-Mines entities. This includes data requested for third-party surveys, requests from outside vendors, professional societies, required reporting requirements, or accrediting agencies.

## Appendix A: Business Domains and Applicable Data Trustees

**Institutional Administration:** COVID, IPEDS, SURDS, External Reporting, External Surveys, Marketing and Communications, Institutional Equity and Title IX Records, Preservation of Evidence Directive (PED), Learning Management Systems

- Data Trustee: CIO

**Research Administration:** Proposals, Awards, Compliance Records, Patent and Invention Information, Other Research Related Data

- Data Trustee: Director of Research Administration

**Student Administration:** Admission and Recruitment Records, Student Enrollment Records, Student Educational Transfer Records, Student Academic and Retention History, Financial Aid Records, Course Records, Degree Audit Records, Student Veteran Benefits, Release of Information, and Parent related Records

- Data Trustee: Associate Provost for Enrollment Management

**Student Life Administration:** Athletics Records, Public Safety/Police Records, Student Complaints, Student Disciplinary Records, Student Health Records, Student Counseling Records, Student Case Management (CARE) records, Student Activity and Student Organization Records, Housing Records, Student Disability Records, Student Career Outcomes, Academic Advising Records, Meal Plan/Dining Records, ID Cards, Event Records, Blaster Card Access Records.

- Data Trustee: Associate Vice President for Student Life

**Employee Information:** Personnel Records (includes performance management, conflict of interest, job history, compensation and incentives, payroll history, employee medical information, training records, employee relations/complaint information), Employment Applications, Training, HR Compliance Records.

- Data Trustee: Human Resources Director

**Financial Resources:** General Ledger, Credit Card/PCI, Vendor, Accounts Receivable, Student Billing, Payroll, Student Contracts, Student Sponsor Data, Debt, Investments, Non-Research Revenue, Procurement, Construction Contracts, Student Accounts Records, Purchasing, Capital Inventory Records, I-9 documentation, unemployment information, banking information, W2/W4 information.

- Data Trustee: Controller

**Budget Resources:** Budget, Employee Position Budget

- Data Trustee: Executive Director for Financial Planning

**Academic Affairs:** ABET, HLC, Assessment, Faculty Tenure, Faculty Rank and Faculty Performance

- Data Trustee: Associate Provost for Operations

**Extended Studies and International Information:** CPES, SEVIS, and other International Student data collected by this Data Trustee's Business Domain.

- Data Trustee: Vice President of Global Initiatives

**Campus Resources, Services and Facilities:** Campus Facilities Records and Parking Records

- Data Trustee: CIO