



CSM Administrative Data Access Policy
Guidelines and Procedures for Handling, Using, and Securing Institutional Data

1) Definitions

- a) **Administrative Data:** Administrative data are defined to be the collection of data elements used by the School to help it accomplish its business needs. Examples include, but are not limited to, data elements in the Student Information System, Finance System, HR/Payroll System, Environmental Health Inventory System, Plant Work Order System, etc.. Administrative data also include any personal, private, or confidential data elements collected via any other means (e.g. questionnaire, survey, application, etc.) Administrative data are organized into three categories:
- i) **Restricted Data:** Restricted data are defined to be those data elements that are governed or restricted in some manner by a federal or state statute, rule, or requirement. Examples include, but are not limited to, social security number, grades, financial, and enrollment information. Also, directory information, as defined in the undergraduate and graduate bulletins, can be restricted at the request of a student.
 - ii) **Internal/Confidential Data:** Internal data are those data elements collected and maintained about an individual that may be required to conduct School business but are not necessarily legally protected. Such data elements are considered to be confidential and are accessed on a “need-to-know” basis. With the exception of the directory information identified in the undergraduate and graduate bulletins, all data elements that describe an individual are considered to be internal/confidential. Students, however, can elect to designate directory information as restricted data. Lists of otherwise public data (usually directory information) such as e-mail, telephone, or home address lists are also considered internal/confidential.
 - iii) **Public Data:** Data that can be freely disseminated to the public at the discretion of an appropriate School official. Such data may typically be accessed by the public without filing an open records request but a formal request may be necessary in some circumstances. These data are rarely about an individual and are often aggregated or summarized. Examples may be summarized data that would go into a press release or announcement prepared by the appropriate office.
- b) **Data Steward:** A “data steward” is defined to be the position responsible for defining, managing, and maintaining the integrity, security, and accuracy of specific data elements collected by the institution in various forms, generally stored in electronic institutional databases, and used as the official data source by many departments of the institution to conduct official business. Examples of “data stewards” may include the Payroll Manager as it relates to payroll data, Human Resource Specialists, Registrar, the Controller and others, as well as their respective designees.
- c) **System Owner:** A “system owner” is defined to be the position responsible for the oversight and general operation of an administrative application system that serves a broad section of the university community. The position of system owners and data stewards may often overlap. Examples of system owners include the Registrar for the Student System, the Controller for Finance, the Director of Human Resources for HR-related systems, the Financial Aid Director for Financial Aid, the Plant Facilities Director for HVAC controls, and so forth.

2) Access to Administrative Data

Data created, collected, and maintained by the Colorado School of Mines are required to conduct institutional business. Colorado School of Mines regards the security and confidentiality of its business data and information to be of significant importance. Each employee, consultant, student, or person granted access to administrative data and information, whether in electronic, paper, or other format, holds a position of trust and must preserve the security and confidentiality of the information he/she uses. Access to administrative data:

- a) is restricted to individuals whose job duties require it;
- b) is granted only to fulfill the specific functions required to perform a specific job;

- c) must be approved by both the employee's department head and the system owner before Information Services (IS) will provide the requested credentials.

System owners are encouraged to use the principle of least privilege when authorizing access to data for which they are responsible. In some cases, system owners may require prospective users to attend formal training before access will be granted.

3) Use of Administrative Data

All administrative data are the property of the Colorado School of Mines and may only be used by individuals for the CSM business which they are authorized to conduct. Institutional research as it relates to the role or responsibilities of one's position is considered to be a routine, and therefore acceptable use, of administrative data. Specific non-School business use of administrative data may be authorized under other official School policy or with the written permission of the "system owner" responsible for housing and maintaining the data. Unless specifically permitted by another official School policy or by written permission of the "system owner", the use of administrative data for personal gain, curiosity, academic research, or for another's personal gain, curiosity, or academic research is prohibited.

4) Sharing and Release of Administrative Data

- a) Within the institution, employees may share or disseminate administrative data to other employees who have a legitimate need to access or use the information.
- b) Employees may release appropriate data, if such activity is defined to be part of their job and at the direction of their supervisor, to honor requests from appropriate state or federal agencies such as CCHE, legislative bodies, Governor's Office, NSF, ONR, and other applicable agencies.
- c) Due to the complex nature of laws governing the use of certain types of data, as well as the sometimes complex nature of the data themselves, it is in the best interest of the institution and its employees that administrative data generally be formally released outside the institution only by authorized individuals such as those who are designated as system owners or data stewards, as appropriate. CSM's Privacy Policy can be found at http://www.mines.edu/all_about/policy/csmprivacypolicyinfo.html. It is the data user's responsibility to access and use administrative data in accordance with CSM policy and State and Federal laws. If in doubt, contact your supervisor or the Office of Legal Services. Specifically, for each type of data:
 - i) **Restricted Data:** Requests for restricted data are to be referred to the office authorized to respond to such requests and are to be released only by authorized personnel in accordance with applicable law and University policy. The use of much of CSM's administrative data is covered by State statute and Federal law (e.g. Health Insurance Portability and Privacy Act, Social Security Act, and many others) and may be defined as personal, private, or confidential. Employee personnel information, payroll data, etc. are considered high risk data because it could cause damage to CSM and employees if disclosed, misused, or modified. Student data likewise are considered high risk and covered by the Family Educational Rights and Privacy Act (FERPA) as amended. Faculty and others who have access to student educational records may not release any information contained in a student's educational record to a third party without written consent from the student. There are some exceptions to this rule, but requests for student information from outside CSM (including requests from the student's parent) are to be referred to either the Registrar's Office or the Office of Legal Services.
 - ii) **Internal / Confidential Data:** Requests for these data should be referred to the office authorized to respond to such requests and are to be released only by authorized personnel in accordance with University policy.
 - iii) **Public Data:** To present and interpret institutional data correctly, disclosure of even public data should be done by an appropriate University official. Public data may be disseminated freely by such an official.

5) Administrative Data User Responsibilities

As a condition of access, administrative data users agree to adhere to the following terms and conditions, as applicable, when they access or are in possession of administrative data of any kind. These requirements reflect best practices used in the industry today and may be amended in the future as needs change. Administrative data users are required to acknowledge they will adhere to these requirements to the best of their ability when they sign the System Application/Authorization Request form for the system to which they require access. Specifically, an individual given access to CSM administrative data in any format (printed, electronic, or any other media) acknowledges an understanding of and agrees to adhere to the following:

- a) Security is to be maintained by not providing anyone else access to or use of administrative data or data systems. As noted below, you are responsible for all activity that occurs under your computer accounts so you should not share your username(s) or password(s) with anyone else. This includes your supervisor, co-workers, or colleagues at CSM or anywhere else. Further, you may only share administrative data, in any format, with other employees who are authorized or required by their job function to see the data.
- b) Student access to Internet Native Banner is generally discouraged. Offices that need student employee access must request individual access for each student according to number 1 above, and must insure that the student has received the appropriate training. Shared usernames for use by multiple student employees in an office will generally not be granted in any system or application. The difficulty this policy could create is understood and requests for student employee access when needed will be expedited. Departments must inform IS immediately when an individual student or any other employee no longer needs access so their username can be disabled.
- c) The username and password combination is considered equivalent to a signature and individual account owners are responsible for activities that occur under that username. Many systems log activities performed by an individual username.
- d) Proper password security to all systems is to be maintained by creating passwords that are difficult to guess, are changed at least every six months, and not written down, stored or emailed in un-encrypted file or email systems, and never revealed to anyone.
- e) Workstations that connect to administrative systems are to be properly maintained and managed to prevent problems that could affect the entire CSM computing environment. Workstations should run current anti-virus and spyware software, and system or applications patches supplied by vendors should be applied regularly. See your computer support specialist for assistance with these requirements.
- f) You are expected to maintain physical workstation security by not leaving a workstation unattended while logged into a CSM administrative system unless a password-protected screen saver is in effect. (This is true with all systems, but particularly true with Banner since it does not provide an automatic logout as did the Plus systems.)
- g) Storing administrative and other sensitive data on the **local** hard disk of any computer or storage system, including office workstations, laptop computers, PDAs, telephones, CDs, DVDs, diskettes, USB memory devices, and other portable media expands the potential for the data to be fraudulently accessed and misused. Users of administrative and private or otherwise sensitive information (see #4 above) are expected to take special precautions to protect the security and integrity of data to which they have access in any form. Administrative data (see #1 above) downloaded or entered into a local application (spreadsheet, word processor, email, etc.) should be handled by all employees according to the following best practices:
 - i) Data should be stored on hardened, protected, and managed network file systems using security settings which prevent anyone other than the data user (and system administrators) from accessing the data. Members of the INFO_SERVICES domain (and users who logon through other domains) should store files on the centrally managed file system server for that domain.

- ii) Data should not be stored on the local hard drive of an office, laptop, or other personal computer unless the file and file system are encrypted. Methods to escrow encryption keys are being evaluated and escrow will be offered and possibly required in the future. An individual file can also be password protected but this protection is relatively weak. Storing files on a centrally-managed file server such as the INFO_SERVICES domain is the preferred storage method, however.
- iii) Data should not be moved to any external media such as a USB memory key, CD, DVD, diskette, or similar unless the files placed on that media are encrypted or at least password protected. Encryption is the preferred method and should be combined with password protection if possible. Many encryption packages can be found on the internet or users may purchase removable USB devices which automatically encrypt data such as those found at <http://www.kanguru.com/aesmicrodrive.html> and elsewhere. Users will be held professionally accountable in the event of loss or disclosure of CSM data due to loss or theft of a laptop, pda, or other device.

See your computer support specialist for assistance in designing a procedure that will work in your office which complies with the above requirements.

- h) Users are expected to comply with the sharing and release of administrative requirements described in section 4 of this document. All requests to provide data to someone outside the institution should be referred to the appropriate office.
 - i) When finished working with administrative data on a local computer system, files should be deleted and purged.
 - j) When finished using administrative data in printed document form that are not be filed for long-term access, documents should be shredded.
- 6) Suspected security violations are to be reported to the department head, the system/module owner, and the Director of Information Services as soon as practically possible when an event involving administrative data security or privacy is thought to have occurred or is occurring.
 - 7) The privacy and confidentiality of all accessible data shall be maintained at all times. Unauthorized disclosure of personal/confidential information is a violation of this policy and may result in disciplinary, civil, and/or criminal actions against an individual.
 - 8) Banner systems users who are authorized to enter or modify data in Banner databases must read and agree to adhere to the Data Standards handbook which describes the approved data element formats and requirements for entering data into Banner. User's must follow these standards and may not create new data element values or definitions.
 - 9) CSM will take any and all actions it deems necessary to resolve violations of this policy.