Requirements for the Creation and the Maintenance of Student Data in Electronic Repositories

Effective Date: December 2009

Applies to: All users of University shared student data repositories that include data drawn from the Integrated Student Information Systems (ISIS), as well as any other source of student data.

Prepared by: Student Data Access Group (DAG)

Approved by: SIS Executive Steering Committee

Distribution: Via Campus IT Policy Councils and Other Campus Committees

PURPOSE OF THE GUIDELINES

These guidelines establish expectations regarding the creation and maintenance of student data in support of the operation and management of academic, student service, and other University programs, while also adhering to university policies regarding data security, data access, the privacy of student data, and promoting the integrity and correct interpretation of student data. Student data will be made available to faculty and staff of the University of Colorado who demonstrate a legitimate educational interest and can demonstrate proper security controls are in place to protect this data.

DEFINITIONS

Electronic University Student Data Repository – Any collection of data about students or prospective students of the University of Colorado that is created by a university employee for academic, student services, or other University purposes and is maintained in or derived from an electronic medium. Examples include an electronic database, an electronic spreadsheet, and an electronic text file.

Shared Student Data repository – an Electronic University Student Data Repository that represents a shared asset, utilized by multiple organizations and data users to achieve various educational purposes or objectives. Interest in data quality, security, and control is shared amongst user organizations.

ISIS – Integrated Student Information System. ISIS refers to the university's central student information system and its related satellite systems, including but not limited to the Customer Relationship Management (CRM) system, the DARS degree audit system, the Singularity Document Management System, the Central Information Warehouse (CIW), the enterprise student/faculty/staff portal, and other supporting infrastructure elements including the Master Data Management (MDM) system.

Data Owner: The party or entity identified with and widely recognized to have primary authority and decision responsibility over a particular collection of university data. Data owners are accountable to manage, protect, and ensure the integrity and usefulness of university data. Data owners have the primary responsibility to ensure the university is following its policies and is in compliance with federal and state laws and regulations. Data owners typically are associated with the business functions of an organization rather than technology functions.

Data Custodian: Any party charged with managing a data collection for a data owner. Custodians typically have control over a data asset's disposition, whether stored (at rest), in transit, or during creation. Custodians will often have modification or distribution privileges. Data custodians carry a significant responsibility to protect data and prevent unauthorized use. Data custodians are often data providers to data users. Data owners or data stewards may also exercise custodial roles and responsibilities. Data custodians typically are associated with IT units within the university, either central IT organizations or IT offices within academic and administrative units.

Data Steward: A data steward is a party or entity possessing delegated authority to act on a data owner's behalf. Data Stewards will often have data custodial responsibilities, but are distinguished from custodians by delegated decision making authority regarding the data. Data stewards may represent data owners in policy discussions, architectural discussions, or in decision making forums. Data Stewards actively participate in processes that establish business-context and quality definition for data elements. Data Stewards are more likely to be associated with business functions than IT functions.

Data User: Any person or party that utilizes university data to perform his or her job responsibilities. To the degree that a data user controls the disposition of university data, he or she has responsibility for the custodial care of that data. Data users share responsibility in helping data stewards and custodians manage and protect data by understanding and following the IT security policies of the university related to data use.

SCOPE

These guidelines appliy to all university faculty and staff who:

- Create a shared student data repository from any source, including the university's ISIS and related systems, campus student data repository, or collect data based upon the voluntary release of information provided by University of Colorado students. In other words, create a shared data repository through collecting data from students who volunteer their data based on a request, a survey, or other means.

Examples of shared student data repositories include:

- ISIS
- CIW
- DARS
- Campus Learning Management Systems
- Campus Directories
- Advising systems
- Gradebooks if shared
- Transaction systems, such as those used by Facilities Management, Resident Halls, Libraries, Parking Management, or Athletics, where personally identifiable information about students is stored and processed.
- Data reporting and analysis systems that contain personally identifiable student data

RELATED DOCUMENTS

- All University of Colorado IT Security Policies (available at https://www.cu.edu/content/policies-and-procedures), and especially https://www.cusys.edu/policies/policies/IT_IT-Service-Provider-Security.html
- Family Educational Rights and Privacy Act of 1974 (FERPA)
- All related UIS and campus IT security policies and access procedures.

GUIDELINES

An academic or administrative unit will be permitted to create and maintain a *shared student data repository* when it can (1) demonstrate a legitimate educational interest for access to this data, and (2) can demonstrate to campus information technology security authorities that proper security controls are in place to protect this data. The unit head, with assistance from the unit's data custodian, will complete the "Application to Create a Shared Student Data Repository" and the campus IT security controls assessment questionnaire. After approval has been granted, the unit head must consent to a review of security practices and inspection of security controls for the system and/or database.

Proper security controls are defined in the university's APS and related procedures, and in campus IT security policies and procedures. The campus IT Security Principal will assess the IT security controls based on information provided in the assessment questionnaire. The IT Security Principal will provide an overall assessment to the data owner. The Security Principal will report significant weaknesses to the unit head and data custodian. The data custodian will then need to prepare a vulnerability mitigation plan and submit it to the Security Principal. If significant weaknesses are found, the data owner reserves the right to deny access to the data.

All users of student data must adhere to the requirements of FERPA. The unit head must make sure that users can demonstrate an understanding of the structure and content of the student data that is to be stored; their responsibility to protect the integrity and confidentiality of the data; and the correct use of tools for accessing and analyzing the data. Permission to create a data repository will only be granted after expectations are met for managing a student data repository. Usage will be monitored through periodic review.

Student data drawn from these student data repositories may only be shared with other university employees when there is an educational interest, as defined in the FERPA regulations, for doing so. Data can be shared with non-university personnel or organizations when there is an educational interest, as defined in the FERPA regulations for doing so. Before sharing data with non-university organizations, contact the data owner of the data.

Sharing is different from propagation of student data. Any propagation of student data means that a new student data repository is being created. Any request for propagating data from a unit's shared repository must be referred to the proper data owner. Academic and administrative units should not proceed with data propagation until permission has been granted from the Data Owner.

Only University faculty and staff who have an educational interest as defined by FERPA may access the data in any student data repository. In addition, all university faculty and staff who access student data via student data repositories are required to first complete the University's

FERPA training requirements and any additional training required by university IT security policies.

RESPONSIBILITIES OF USERS AND SANCTIONS FOR INAPPROPRIATE USE

Report Security Violations, Malfunctions and Weaknesses – any security related event must be reported if it is known or suspected. Any inappropriate, unethical or illegal activities involving university IT resources must be reported to campus IT security principals. If unsure of the local incident reporting process, users shall call the appropriate IT service center or help desk.

Inappropriate sharing of data from a student data repository or persistent improper release, misuse or misinterpretation of such data will be grounds for penalties such as suspension of access privileges, a letter of reprimand, an unsatisfactory performance evaluation, employment termination, and/or accountability in a court of law.

The responsibility for enforcement of all requirements of these guidelines fall on the data custodian of the data repository.