



Institutional Data Procedures: Data Classification and Access Control

October 18, 2007

I. Data Classification

Data classification provides a basis for understanding and managing institutional data based on the level of criticality and required confidentiality of the data. Accurate classification provides the basis to apply an appropriate level of security to institutional data. As part of the data classification process, data stewards will assign each data element and each data view in institutional data to one of three categories: public, limited access and restricted. These classifications are the same as used in The State of Ohio's family of Information Technology Policies and Administrative Rules. Data stewards will then be responsible for reviewing these data classifications as required and at a minimum every two years and maintaining a history of previous versions.

By default, all institutional data will be designated as internal data for use within the university or to satisfy external reporting requirements to the Ohio Board of Regents, and to State, Federal, or other external agencies. This data will be classified as Limited Access Institutional Data and University employees will have access to these data for use in the conduct of university business. These data, while available within the university, are not designated as open to the general public unless otherwise required by law.

Data Stewards may assign non-default Public or Restricted classifications to data based on the needs of the university as well as applicable laws and regulations

Note: In some circumstances, as long as specific identifying data elements are removed, a data view may include elements of institutional data that would otherwise be limited access or restricted.

A. Public Data

Where appropriate, data stewards may identify institutional data elements that are intended for public use or have no access restrictions as available to the general public. These data will be designated as Public Data.

Examples: High-level Enrollment Statistics, Course Catalog, Current Funds Budget, Financial Statements, and data on web sites intended for the general public.

B. Limited Access Data

While Limited Access is the default, where necessary, data stewards may specify institutional data elements for which users must obtain specific authorization to access since the data's unauthorized disclosure, alteration, or destruction will cause perceivable damage to the university.

Note: All institutional data in the enterprise-level administrative systems is classified as Limited Access unless otherwise indicated.



Institutional Data Procedures: Data Classification and Access Control

October 18, 2007

Examples: Date of Birth, Ethnicity, Purchasing Data

C. Restricted Data

Where required, data stewards may identify institutional data elements as **restricted**, for which the highest levels of protection should apply, both internally and externally, due to the risk or harm that may result from disclosure or inappropriate use. This includes information protected by law or regulation whose improper use or disclosure could:

1. Adversely affect the ability of the university to accomplish its mission
2. Lead to the possibility of identity thief by release of personally identifiable information of university constituents
3. Put the university into a state of non-compliance with various state and federal regulations such as FERPA, HIPAA, GLBA
4. Put the university into a state of non-compliance with contractual obligations such as payment card industry data security standards

The specification of data as protected should include reference to the legal or externally imposed constraint that requires this restriction, the categories of users typically given access to the data, and under what conditions or restrictions access is typically given.

Data stewards and data custodians are responsible for identifying and implementing safeguards for Restricted Data. If the applicable laws and regulations or University Computer Security Standards do not specify how to adequately safeguard the restricted data, the Data Steward is responsible for developing safeguards based on information security best practice working in cooperation with the Office of the CIO and Legal Affairs. In some cases, multiple data stewards may collect and maintain the same restricted data element. In these cases, these data stewards must work together to implement a common set of safeguards.

Data stewards are responsible for communicating and providing education on the required minimum safeguards for protected data to authorized end users and data custodians.

Examples: Social Security Numbers, Personal Financial Data protected by GLBA, Credit Card Information protected by contractual obligations under PCI standards, security data, all data exempt from disclosure under Ohio's Public Records Laws unless the exemption is waived by the university.

II. Data Access Control



Institutional Data Procedures: Data Classification and Access Control

October 18, 2007

Data stewards must work with data custodians to develop and implement policies and procedures for requesting and maintaining access to institutional data. These policies and procedures shall be developed taking into account the risk associated with the specific data and/or system being accessed. The following minimum standards must be incorporated into the individual data access policies and procedures for systems and facilities containing Restricted and Limited Access data:

- A. Anyone with access to Restricted or Limited Access Institutional Data shall have unique and individual user credentials such as a user id and password.
- B. Access shall be deactivated after a period of inactivity not to exceed twelve months.
- C. Terminated employees shall lose access as of their termination date.
- D. The data access request process shall be formalized and auditable. The request process must include appropriate approvals, a description of the specific data requested, the level of access requested (read, write), and the purpose for accessing the data. Data access requests should be maintained in order to support the need to audit data access permissions throughout the complete data access lifecycle (creation through termination).
- E. Once data access is approved for a data user or data custodian, data stewards are responsible for providing access to the Institutional Data Policy and the following information specific to the data being requested: 1) data documentation and usage guidelines, 2) the data classification policy including information on associated state and federal regulations, and 3) required minimum safeguards for protected data.
- F. A robust authentication process in compliance with university computer security standards and consistent with the level of risk associated with unauthorized access is required for access to all limited Access and Restricted data.
- G. Maintain and monitor user access and login information .
- H. Data access processes, procedures and authorizations must be reviewed on an annual basis by each data steward to ensure that access remains appropriate.