UNC INFORMATION TECHNOLOGY SERVICES

Responsible University Officer
Chief Information Officer

Responsible Office
Information Technology Services

Institutional Data Governance Policy

Policy Statement

Institutional Data is a strategic asset of the University. As such, it is important that it be managed according to sound data governance procedures.

This policy serves three primary purposes:

1. It assigns stewardship responsibilities for University administrative data;

2. It establishes standards for the custodianship of such data; and

3. It empowers the Institutional Data Coordinating Committee to establish standards and/or procedures for storage, retrieval, destruction, backup, and access as needed to ensure proper management and protection of Institutional Data.

The Vice Chancellor for Information Technology and Chief Information Officer has authority and responsibility for preserving the security and integrity of Institutional Data. Proper stewardship and custodianship of University Institutional Data will facilitate access to data that supports the work of those with official educational or administrative responsibilities within the institution and will inform users of data of their responsibilities.

Institutional Data is available to individuals carrying out their University work responsibilities on an as needed basis. An individual interested in utilizing Institutional Data for any other purpose must request the Institutional Data through a public records request. The Public Records Officer and the Office of University Counsel have responsibility for interpreting the laws governing data access and related issues.

Note: Nothing in this policy precludes or addresses the release of Institutional Data to external organizations, governmental agencies, or authorized individuals as required by legislation, regulation, or other legal vehicle.

Scope

This policy establishes the framework of standards and guidelines to be followed in the management of Institutional Data, including procedures that govern the creation of data architectures and access mechanisms.

This policy addresses, but is not limited to, machine-readable data, data in electronic communication systems, data in print, and backup and archived data on all media.

Audience

This policy applies to Stewards, Custodians, and Consumer/Users of Institutional Data, as defined below.

Definitions

- **Access:** The right to read, enter, copy, query, download, or update data.
- **Data:** The representation of discrete facts; any information in electronic or audio-visual format, or any hardware or software that enables the storage and use of such information. The SAA Glossary of Archival and Records Terminology (http://www.archivists.org/glossary/): Facts, ideas, or discrete pieces of information, especially when in the form originally collected and unanalyzed.
- **Consumers/Users:** Employees or agents of the University who access Institutional Data in performance of their assigned duties.
- **Custodians:** University officials and their staff who have operational-level responsibility for the capture, maintenance, dissemination, and storage of Institutional Data.
- **Stewards:** Senior University officials whose areas have responsibility for managing a segment of the University's Institutional Data resources.
- **Institutional Data:** Institutional Data is a subset of the University's information resources and administrative records and includes any information in print, electronic, or audio-visual format that meets the following criteria:
  - Acquired and/or maintained by University employees in performance of official administrative job duties;
  - Created or updated via use of a University enterprise system or used to update data in an enterprise system;
  - Relevant to planning, managing, operating, or auditing a major function at the University;
  - Referenced or required for use by more than one organizational unit; and
  - Included in official University administrative reports or official University records.
- **Institutional Data Coordinating Committee (IDCC):** The committee that establishes overall policy and guidelines for the management of and access to the University's Institutional Data in accordance with existing University policies and applicable law and regulation. The role of the IDCC is described more fully below.
- **Institutional Data Model:** A framework that documents the data entities that comprise the Institutional Database and the relationships among those entities.

- **Record:** Data or information in a fixed form that is created or received in the course of individual or institutional activity and set aside (preserved) as evidence of that activity for future reference.

Types of Institutional Data

- **Alumni Affairs and Development:** Includes all aspects of alumni and development data.
- **Facilities:** Includes the facilities services data of the University including space-planning data, construction, maintenance and operational data, reservations and physical-descriptive data.
- **Financial:** Data related to the management of fiscal resources of the University including accounting, accounts payable, accounts receivable, budgeting, capital assets, investments, inventory, loans, payroll information, purchasing, risk management, and treasury.
- **Human Resources:** Supports the management of employee resources of the University including employee demographics, benefits, retirement and EEO data, vitas, employee evaluations, and promotion and disciplinary data. Note that FERPA applies to the HR records of students whose enrollment is a contingency of their employment (TAs, work study awards, etc.) Human Resources data can be both part of the student record and the Human Resources record.
- **Information Technology:** Supports the provisioning and management of the technology infrastructure provided by Information Technology Services.
- **Library and Information Resource:** Supports the management activities and information-resource-collection activities of the University libraries including databases of purchased and locally produced information and all files of University archives and other special collections.
- **Organizational:** Reflects the internal organizational structure of the University and identifies hierarchical relationships among individual entities. Supports the ability to organize and aggregate/disaggregate various kinds of institutional data using standard reporting structures adopted to meet business or functional needs. Data may include level (vice chancellor, division, department, etc.), parent/child relationships, official name, reporting abbreviations, codes and account numbers, type of organization (academic vs. administrative, Health vs. Academic Affairs, etc.), and status (active/inactive).
- **Person Registry:** Supports the management of identity and authentication for individuals associated with the University including the creation of unique data elements (e.g., PID and UNC OneCard) that provide unambiguous identification and resolution for merging of identity records. Person-registry data can be used to provision other applications that are managing privileges to authorized individuals or groups.

- **Research:** Includes records that represent grants & contracts (proposals and awards) the University has received and executed including dates, amounts, responsible units, project teams, percent effort, and others as appropriate. Proposal narratives and research results are excluded.
- **Student:** Supports all phases of a student's relationship with the University from expression of interest through alumni status except as noted elsewhere. This includes, but is not restricted to, demographic data; academic, disciplinary, and medical records; course information, admissions data, housing, financial aid, and employment with the University, which is dependent on student status.

- **Exclusions:** Specifically excluded from the definition of Institutional Data are: personal medical (other than certain student health records), psychiatric, or psychological data for employees, students, and clinic patients; sole possession notes and records that are the personal property of individuals in the University community; research notes, data and materials; data that results from sponsored research projects; and instructional notes and materials.

Governance Roles and Responsibilities

No one person, department, division, school, or group "owns" Institutional Data, even though specific units bear some responsibility for certain data. The University owns the data (or in some cases, such as with Social Security numbers, is the custodian of data), but a specific person in the form of the Steward has ultimate responsibility to define management of the assigned data set within the scope of legal and regulatory obligations. The roles and responsibilities outlined below will govern management, access, and accountability for Institutional Data and will be assigned by the Institutional Data Coordinating Committee.

1. Institutional Data Coordinating Committee (IDCC)

The IDCC is an official University committee that is part of the University's IT governance structure and reports to the Provost on the development and enforcement of the University's Institutional Data Governance Policy. The Provost appoints Committee members, who include representatives from University Counsel, University Archives, Institutional Research and Assessment, Information Technology Services, Information Technology Security, and senior University management. The IDCC may create subcommittees and task forces as needed to carry out its responsibilities.

Other Committee responsibilities include:

Access: Defining a single set of procedures for requesting permission to access data elements in Institutional Databases and, in cooperation with Stewards, documenting these common data-access request procedures.

Conflict Resolution: Resolving conflicts in the definition of centrally-used administrative data attributes, data policy, and levels of access. Resolving issues with regard to standard definitions for data elements that cross stewardship boundaries.

Data Administration: Applying formal guidelines and tools to manage the University's data resources. Overseeing the administration and management of all Institutional Data.

Data Management: Establishing policies and procedures that manage Institutional Data as a University resource and communicating them to the University community.

- Establishing specific goals, objectives, and action plans to implement the policy and monitor progress in its implementation.
- Identifying data entities and data sources that comprise Institutional Data. As this is an ongoing process, the committee will add data entities and sources to the scope of Institutional Data as circumstances require.
- Prioritizing the management of Institutional Data including identifying which data is most critical and assigning management priorities to all data entities and sources.
- Considering delivery modes for transmitting Institutional Data.
- In consultation with University Counsel and the Information Security Office, making policy decisions related to contracts with vendors for products that will intersect with University databases, including third-party contracts for secondary systems that share data housed in the primary technological architecture.

Institutional Data Model: Overseeing the establishment and maintenance of the Institutional Data model and defining the standard for documentation of data elements.

Shared-Data Management: Defining attributes and assigning maintenance responsibilities for data retention, disposition, and preservation. Access to Institutional Data which is a public record should be managed in accordance with the North Carolina Public Records Act The retention and disposition of Institutional Data should conform to the policies of University Archives and Records Management Services.

2. Stewards

By virtue of their positions, Stewards of Institutional Data have the primary administrative and management responsibilities for segments of Institutional Data within their functional areas. For example, the Vice Chancellor for Human Resources has stewardship responsibility for HR data.

Stewards of Institutional Data interpret policy, define procedures pertaining to the use and release of the data for which they are responsible, and ensure the feasibility of acting on those procedures. Stewards are responsible for defining procedures and making policy interpretations for their business unit(s). Any such business-unit-specific items must, at minimum, meet University policy standards. They are responsible for coordinating their work with other University offices associated with the management and security of data, such as University Counsel, the Information Security Officer, and Information Technology Services (ITS). Specific responsibilities include:

Access: Approving requests for access to Institutional Data within their functional area, specifying the appropriate access procedure, and ensuring appropriate access rights and permissions according to classification of data. In some cases, this will require working closely with the University's Public Records Officer.

Communication: Ensuring that Consumer/Users of the data for which the Stewards are responsible are aware of information-handling procedures.

Compliance: The Steward is ultimately responsible for compliance with applicable University policies and legal and regulatory requirements. Stewards must be knowledgeable about applicable laws and regulations to the extent necessary to carry out the stewardship role. Stewards must take appropriate action if incidents violating any of the above policies or requirements occur.

Consultation: Providing consulting services as needed to assist Custodians and data Consumer/Users in the interpretation and use of data elements for which the Steward is responsible.

Coordination: Ensuring that, where required, Information Security Liaisons are designated for their respective business unit, specifying data management and protections requirements to Custodians of Institutional Data.

Data Classification: Classifying each data element according to University definition - Sensitive (high risk) and Public (low risk).

Documentation: Ensuring that documentation exists for each data element to

include, at a minimum, data source, data provenance, data element business name, and data element definition.

Data Manipulation, Extracting, and Reporting: Ensuring proper use of Institutional Data and recommending appropriate policies regarding the manipulation or reporting of Institutional Data elements and implementing business unit procedures to carry out these policies.

Data Quality, Integrity, and Correction: Ensuring the accuracy and quality of data (access control, backup, etc.) and implementing programs for data quality improvement.

- Developing procedures for standardizing code values and coordinating maintenance of look-up tables used for Institutional Data.
- Determining update precedence when multiple sources for data exist.
- Determining the most reliable source for data.

Data Lifecycle and Retention: Ensuring appropriate generation, use, retention, disposal, etc., of data and information consistent with University Policies, among them the Information Security Policy and standards for disposal.

Data Stewardship: Other responsibilities as necessary, including exercise of due care in the selection of Custodians of Institutional Data, to ensure these responsibilities are adequately and consistently executed.

Data Storage: Documenting official storage locations and determining archiving and retention requirements for data elements.

Education: Ensuring that education to employees responsible for managing the data is provided in data retention, data handling, and data security.

Policy Implementation: Establishing specific goals, objectives, and procedures to implement the policy and monitor progress toward implementation.

3. Custodians

Stewards of Institutional Data may appoint Custodians to assist with data-administration activities. A Custodian of Institutional Data is given specified responsibilities and receives guidance for appropriate and secure data handling from the Stewards. A Custodian has the responsibility for the day-to-day maintenance and protection of data. Specific responsibilities also include:

Access: Implementing procedures as defined by the IDCC and Stewards to grant access to Institutional Data to Consumer/Users.

Coordination: With guidance from the respective Stewards and in collaboration with technical support staff and University Counsel, Custodians recommend appropriate IT procedures that satisfy specified information security requirements including legal and compliance obligations as well as applicable University policies.

Data Collection and Maintenance: Collecting and maintaining complete, accurate, valid, and timely data for which they are responsible.

Data Security: Administering and monitoring access. In collaboration with technical support staff, defining mitigation and recovery procedures. Reporting any breaches of University information in a timely manner in accordance with the Incident Management Policy. Coordinating data protection with the Information Security Office as necessary.

Documentation: Writing the documentation for each data element based upon stewardship requirements, policy, and best practices. This documentation will include, at a minimum, the data source, data provenance, data element business name, and data element definition.

Education: At the direction of the Steward, providing education in data retention, data handling, and data security to employees responsible for managing the data.

4. Consumer/Users

Consumer/Users are employees or agents of the University who access Institutional Data in performance of their assigned duties. This access includes reading, entering, downloading, copying, querying, or updating data or information.

All data Consumer/Users must adhere to the following:

Confidentiality: Respecting the confidentiality and privacy rights of individuals whose records they may access.

Ethics: Observing the ethical restrictions that apply to data to which they have access.

Policy Adherence: Abiding by applicable laws and University policies with respect to access, use, protection, proper disposal, and disclosure of data.

Responsible Access: Accessing and using Institutional Data only as required in their conduct of University business. Reporting any breaches of University information in a timely manner according to procedures defined in the Incident Management Policy.

Quality Control: Reviewing reports created from data to ensure that the analysis results are accurate and the data has been interpreted correctly.

Institutional Data Governance Procedures

Definitions

Access: The right to read, enter, copy, download, query, or update data.

Data: The representation of discrete facts; any information in electronic or audio-visual format, or any hardware or software that enables the storage and use of such information. The SAA Glossary of Archival and Records Terminology (http://www.archivists.org/glossary/): Facts, ideas, or discrete pieces of information, especially when in the form originally collected and unanalyzed.

Institutional Data: Data that is created, acquired, or maintained by University employees in performance of official administrative job duties.

Institutional Data Coordinating Committee (IDCC): The committee that establishes overall policy and guidelines for the management of and access to the University's Institutional Data in accordance with existing University policies.

Data Classification

Data classifications, outlined in the Information Security Policy, categorize Institutional Data based on the level of potential risk if the data were exposed. A data classification matrix is maintained that includes the security classification of the data and identifies a Steward and Custodian(s) for the data (see example below). Access to data will be granted based on these classifications and the role and job requirements of the requestor.

It is possible for data to be combined or gathered in specific ways that reveal information that might become sensitive in aggregate.

Student Data Classification Matrix (Example)				
Area	**Sub-Area**	**Classification**	**Steward**	**Custodian**
Student	Admissions	Sensitive	TBD	TBD
Student	Student Records	Sensitive	TBD	TBD
Student	Student Finance	Sensitive	TBD	TBD

Student	Financial Aid	Sensitive	TBD	TBD

The above table defines the student data at the highest level. A data classification must always take into account the most sensitive data in the collection. Since the data is currently described in such broad groupings, the risk classification is 'Sensitive.' As the components of each sub-area are further detailed, the classification of the data is adjusted to reflect the appropriate sensitivity of the data.

Consumer/User Data Access

University employees or agents must be granted access to data elements according to the procedures specified by the Steward of that data and consistent with applicable laws and regulations. The detail involved in this process can vary significantly by virtue of the consumer role and the classification of data.

Consumer/Users desiring data shall submit a completed form requesting access and acknowledging responsibility to the Steward of that data. The form contains the appropriate level of approval as determined by the Steward. If approval is granted, the Custodian will enter the Consumer/User's credentials into the system, allowing access. If warranted, the Steward or Custodian will seek additional approvals. The IDCC will set policy for access to Institutional Data.

Appendices

1. Regulations, Statutes and Policies

- UNC Computing Policies (http://help.unc.edu/1688)
- Information Security Policy

Regulations & Statutes

- Americans with Disabilities Act of 1990
- FTC Red Flags Rules
- Family Educational Rights and Privacy Act (FERPA)
- Gramm Leach Bliley Act (GLBA)
- HIPAA Security Rule
- North Carolina Identity Theft Protection Act of 2005
- North Carolina Public Records Law General Statutes 121
- North Carolina Public Records Law General Statutes 132

- North Carolina State Personnel Policies
- Payment Card Industry (PCI) Data Security Standard
- Policy and Procedures on Ethics in Research
- The Electronic Communications Privacy Act of 1986 (ECPA)

2. Contacts

Subject	Contact	Telephone	FAX
Policy Questions	The University's Information Security Office	919-445-9393	919-445-9488
Report a Violation	The University's Information Security Office	919-445-9393	919-445-9488
Request Information Security Consulting	The University's Information Security Office	919-445-9393	919-445-9488
Archives & Records Management	The University's Archive and Records Management Services	919-962-6402	919-962-6401
Public Records Request	The University's Public Records Officer	919-843-1830	919-843-1617

3. History

Effective Date:

Revised Date: 12/01/10