THE UNIVERSITY of NORTH CAROLINA at CHAPEL HILL

Issuing Office
Information Technology Services

Responsible University Officer
Vice Chancellor for Information Technology and Chief Information Officer

UNIVERSITY POLICY

Title

UNIVERSITY OF NORTH CAROLINA AT CHAPEL HILL POLICY ON ENTERPRISE DATA GOVERNANCE

Introduction

PURPOSE

This policy establishes a governance framework designed to promote and safeguard the appropriate and effective use of Enterprise Data.

This governance framework serves three primary purposes:

1. Assigning stewardship, management, and custodianship responsibilities for University Enterprise Data;
2. Empowering the Enterprise Data Coordinating Committee (EDCC) to advise University Constituents about procedures for the effective management and protection of Enterprise Data consistent with the operating needs of the University; and
3. Charging the EDCC with recommending Standards and Procedures related to Enterprise Data governance or changes thereto.

SCOPE OF APPLICABILITY

This policy applies to University Constituents with responsibility for management of University Enterprise Data.

Policy

POLICY STATEMENT

Enterprise Data is a strategic asset of the University. As such, it is important that it be managed according to sound data governance practices and procedures. A description of the types of Enterprise Data to which this Policy applies (e.g., student information, financial information, employee information) is included in the Standard for Enterprise Data Governance. Enterprise Data may include institutional information subject to access and disclosure restrictions set forth in the University's Information Classification Standard. Information identified by this Standard as Tier 2 or 3 (Sensitive Information) must be particularly protected.

Proper stewardship and custodianship of University Enterprise Data facilitates access to data by those with educational or administrative responsibilities within the institution. This Policy, the Standard for Enterprise Data Governance, and other Standards and Procedures which may be established under the authority of the Vice Chancellor for Information Technology and Chief Information Officer (CIO) (in conjunction with other University Officials as appropriate) inform University Constituents of their responsibilities to properly classify, use, protect, and manage that data.

Enterprise Data should generally be available on an as-needed basis to individuals carrying out their University responsibilities, subject to other standards of data access and management that may be established to conform to the requirements of law or for the effective operation of the University and support of its mission. This Policy is intended to complement, not supersede, other relevant policies and laws that may be applicable to Enterprise Data, including but not limited to HIPAA, FERPA and the North Carolina Public Records Law. The Public Records Office, Institutional Privacy Office, Internal Audit, and the Office of University Counsel, as applicable, are responsible for interpreting and applying laws governing data access and related issues.

The **Enterprise Data Coordinating Committee (EDCC)** is a University committee that is part of the University's IT governance structure. The EDCC reports to the CIO on the implementation and development of the University's Enterprise Data Governance Policy and Standard and may recommend the establishment of additional Standards and Procedures for proper governance of Enterprise Data. The CIO appoints EDCC members, who include representatives from the Office of University Counsel, University

Archives, Institutional Research and Assessment, Information Technology Services, Information Security Office, Institutional Privacy Office and senior University management. The CIO and the EDCC may create subcommittees and other administrative working groups to carry out these responsibilities. Specific responsibilities of the EDCC are defined in the Standard for Enterprise Data Governance.

Roles and Responsibilities

The University is the owner of Enterprise Data. Individual departments, units, or schools bear responsibilities for certain subsets of Enterprise Data. Data Trustees, Data Stewards, Data Managers, Data Custodians, and those in Technical roles perform distinct functions and have particular responsibilities for Enterprise Data as described below and in more detail in the Standard for Enterprise Data Governance.

Data Trustees for each broad segment or type of Enterprise Data derive authority from their position within the University. Data Trustee positions are listed in the Standard for Enterprise Data Governance. Data Trustees act as advisors to the EDCC. Data Trustees are responsible for strategic planning, policy, and oversight of the segment of Enterprise Data in their functional areas. Data Trustees or their designees are responsible for establishing procedures and promulgating policies applicable to Enterprise Data applicable to their data segment. Among the roles defined by this Policy, the Data Trustee has the highest level of responsibility for the management of Enterprise Data and to promote proper access, accuracy, privacy, integrity, security and availability of the data for which they have responsibility. Data Trustees have responsibility for the activities of designated Data Stewards, Managers, and Custodians to whom they grant authority and access. Specific responsibilities of Data Trustees are defined in the Standard for Enterprise Data Governance.

Data Stewards, by virtue of their position or delegated authority from Data Trustees, have strategic planning, standard-setting, and oversight responsibilities for Enterprise Data in their functional areas. Data stewards, or their designees, are responsible for evaluating requests for access to or the release of Enterprise Data and recommending policies, standards and procedures to promote proper access, accuracy, privacy, integrity, and availability of the data for which they have responsibility. Data Stewards have overall responsibility for the data in the subsets overseen by all Data Managers and Custodians to whom they have delegated authority and access. Specific responsibilities of Data Stewards are defined in the Standard for Enterprise Data

Governance.

Data Managers are subject matter experts designated by Data Trustees or Stewards and have operational responsibilities for the data in a particular subject area. Data Managers have day-to-day responsibilities for managing administrative processes and establishing business rules for effective data management. The Data Manager may authorize or set constraints on specific uses of data within their data segment by data users outside the units that report to the Data Manager. Data Managers are accountable for the data subsets they manage, whether the data are collected or maintained directly by the Data Manager (or their staff), by data users in other University units or by external parties. Specific responsibilities of Data Managers are defined in the Standard for Enterprise Data Governance

Data Custodians, designated by Data Trustees or Data Stewards, are University employees who have administrative and/or operational responsibilities for Enterprise Data. In many cases, there will be multiple Data Custodians for the same data segments. An enterprise application may have teams of Data Custodians, each responsible for varying functions. Specific responsibilities of Data Custodians are defined in the Standard for Enterprise Data Governance.

Technical Roles

The CIO designates Technical roles for the management and security of data systems and the delegation of authority to individuals in such roles. Those in Technical roles establish goals, objectives and procedures to implement the Policies and Standards applicable to the University network and data systems containing or affecting Enterprise Data. Technical roles coordinate with business units and individuals with administrative responsibilities for Enterprise Data to ensure appropriate access rights and permissions are granted for the use of Enterprise Data. Technical roles facilitate gatekeeper/enforcement functions for access based upon rules provided by or generated in collaboration with those in the business roles, develop and maintain systems, develop and maintain IT systems, provide security and monitoring services, advise the EDCC concerning potential risks to the security of Enterprise Data, and perform technical functions relevant to the management and administration of Enterprise Data. Specific responsibilities of Technical Data roles are defined in the Standard for Enterprise Data Governance.

Definitions

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

Data: The representation of discrete facts; any information in electronic or audiovisual format, and 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.

Enterprise Data: Any data or records created or received by UNC-Chapel Hill employees or other constituents in the performance or transaction of University business except where excluded under this Policy or the Standard on Enterprise Data Governance. Enterprise Data includes, but is not limited to, machine-readable data, data in electronic communication systems, data in print, and backup and archived data on all media.

University Constituents: UNC-Chapel Hill faculty, staff, students, retirees and other affiliates, contractors, distance learners, visiting scholars and others who use or access UNC-Chapel Hill resources.

Related Requirements

EXTERNAL REGULATIONS AND CONSEQUENCES

Americans with Disabilities Act of 1990
FTC Red Flags Rule
Family Educational Rights and Privacy Act (FERPA)
Gramm Leach Bliley Act (GLBA)
HIPAA Privacy Rule
HIPAA Security Rule
HIPAA Breach Notification 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 (DSS)
The Electronic Communications Privacy Act of 1986 (ECPA)

UNIVERSITY POLICIES, STANDARDS, AND PROCEDURES

Standard for Enterprise Data Governance
Data Classification Standard
Information Security Controls Standard
Privacy of Protected Health Information Policy
PHI Confidentiality Statement
University Records and Disposition Schedule

Contact Information

POLICY CONTACT

ITS Policy Office: its_policy@unc.edu

Important Dates

- Effective Date and title of Approver:
  a. Effective Date: December 12, 2010 (Formerly "Institutional Data Governance Policy")
  b. Approver: Chief Information Officer

- Revision and Review Dates, Change notes, title of Reviewer or Approver:
  a. Last Revised Date: January 2, 2018
  b. Revised by: Revised by the Enterprise Data Coordinating Committee to reflect current Data Governance best practices, to adhere to the new University Policy on Policies. Approved by the Vice Chancellor for Information Technology & CIO.
  c. Substantive Revisions:
     i. Complete revision. Moved from three-tier to four-tier governance model, added and defined technical roles, clarified roles and responsibilities.
     ii. Revised by the Enterprise Data Coordinating Committee to reflect current Data Governance best practices, separated into Policy and Standard to adhere to the new University Policy on Policies.