POL 08.00.01
Electronic Information Management and Security Policy

Authority: Chancellor

History:
- First issued: April 19, 2007.
- Revised: September 18, 2009.
- Last revised: February 2, 2018.

Related Policies:
- North Carolina General Statute §14-454 – Accessing Computers
- UNC Policy Manual 1400.2 – Information Security
- US Department of Education Family Educational Rights and Privacy Act Guidance (FERPA)

Additional References:
- UNC Pembroke POL 08.00.04 – Information Classification and Management Policy
- UNC Pembroke POL 08.00.05 – Acceptable Use Policy
- UNC Pembroke Copyright Policy

Contact Information: Associate Vice Chancellor for Technology Resources and CIO, (910.775.4340)

1. PURPOSE

1.1 The University of North Carolina at Pembroke recognizes the strategic value of the data within its information systems. The university also recognizes its responsibility to ensure the appropriate use, security, reliability and integrity of this data; to safeguard it from accidental or unauthorized access, modification, disclosure, use, removal or destruction; and to comply with relevant federal and state legislation.

1.2 This policy will provide the general framework to manage and secure data in university information systems and other electronic data storage areas, including electronic records, reports and documents (hereinafter "University Electronic Data"). This policy is an extension of the Information Classification and Management Policy (POL 08.00.04), and adds further requirements for the management of electronic data.

1.3 The university understands the value of providing ready and efficient access to data in support of university business or academic pursuits. The university will seek to do so within the limits of sound practice as well as federal and state laws.

2. SCOPE

2.1 This policy applies to all University Electronic Data regardless of the manner in which it is collected, used, processed or stored. In particular, it applies to all data stored in both enterprise

and department-level information systems and other data storage systems. It applies regardless of form of the data (such as text, graphics, video, audio, etc.) or the storage media (electronic, CD-ROM, DVD, Cloud, etc.).

2.2 This policy applies to electronic data stored in departmental information systems. In cases where the information system or data storage system is used within a single department, the director or manager of said department shall serve as the Data Steward for said data without further delegation of authority from the Chief Data Steward. Nevertheless, the Data Steward shall follow the remaining stipulations of this policy, and shall observe all restrictions on the access as described hereinafter.

2.3 This policy does not apply to creative and / or scholarly works, including software, art, music, etc., that are addressed by the university's Copyright Policy unless said creative work includes or contains University Electronic Data. In the latter case, this policy shall apply to the University Electronic Data included or contained within the creative work, but not the remaining portions of the creative and / or scholarly work.

2.4 This policy does not apply to electronic data collected, used, processed or stored by the university for which a grant or contractual agreement has assigned ownership of the data to an entity other than the university.

2.5 This policy does not apply to data owned by a separate entity that the university has purchased or leased the right to use.

3. DEFINITIONS

3.1 University Electronic Data – Data in any electronic form collected, processed, stored or distributed by the university or its employees. This term applies to data stored in information systems, and includes administrative and academic data as well as documents and other records such as web sites and email, regardless of the electronic media on which the data is stored.

3.2 Chief Data Steward – The Associate Vice Chancellor for Technology Resources and Chief Information Officer shall serve as the Chief Data Steward (hereinafter "CDS") of the university. The CDS is ultimately responsible for the management of and access to University Electronic Data, including definition and standards for encoding of said data. The CDS is responsible for establishing guidelines for the appointment and responsibilities of Data Stewards and Data Managers.

3.3 Data Stewards – University employees who have delegated authority from the CDS for the management of a particular set of University Electronic Data.

3.4 Data Managers – University employees who have delegated authority from a Data Steward for the management of the University Electronic Data or a portion of the data under the purview of the Data Steward.

3.5 Data Users – Individuals who need and use University Electronic Data as part of their assigned duties or in fulfillment of assigned roles or functions within the university community.

3.6 Access – Access to University Electronic Data includes the ability to use, modify, process, distribute or dispose of information, the information systems or other data storage areas where data is stored.

4. POLICY

4.1 All University Electronic Data is the property of the university, unless the ownership of the data is otherwise identified in this or other university policies. All University Electronic Data must be collected, processed, stored, used and distributed in a manner that complies with applicable federal and state laws as well as accepted industry standards and practices. Insofar as possible, University Electronic Data must be accurate, complete and reliable. University Electronic Data must be kept secure and stored in a controlled location.

4.2 Access to University Electronic Data

4.2.1 The CDS shall oversee management of and access to University Electronic Data and shall delegate authority to Data Stewards to manage access to specific portions of University Electronic Data. The CDS shall establish procedures for the appointment of Data Stewards and Data Managers and for the management of access to University Electronic Data. Said procedures shall provide safeguards for data classified as protected or sensitive under the Information Classification and Management Policy (POL 08.00.04).

4.2.2 The university has designated some University Electronic Data as directory information in accordance with the Family Educational Rights and Privacy Act (FERPA). Directory information may be made available to the general public at any time without additional approval, as described in the then-current university catalog.

4.2.3 Data Users shall observe all applicable federal and state legislation and university policies when accessing University Electronic Data. Data Users shall review and follow any information related to information management and security, including policies, procedures and best practices, as it is made available.

4.2.4 Due to the unique nature of their job duties, select members of the Offices of Institutional Research, Internal Audit, and General Counsel, and the Division of Information Technology shall have special access to all data covered by this policy necessary to perform their duties to the university. Such access must be granted by the CDS.

4.2.5 In these cases, the Director of Institutional Research (hereinafter “DIR”), the Deputy CIO, CISO, Director of Enterprise Applications, or Director of IT Support Services shall approve, in writing, the scope of access to data for their respective staffs.

4.2.6 The Office of Institutional Research may prepare reports or release data to entities, either inside or outside the university, upon the approval of the DIR. However, Institutional Research

shall abide by all federal and state legislation and university policies in these situations, and shall coordinate said release with the appropriate Data Steward or Data Manager.

4.2.7 The Office of Internal Audit may query data in order to verify the accuracy and validity of the data or to complete other audit activities. The Office of Internal Audit may enlist the aid of additional offices as necessary.

4.2.8 The Division of Information Technology (DoIT) may assist other offices in the preparation of reports or data. However, DoIT shall only accept requests for such assistance that have been approved by the appropriate Data Steward, Data Manager or the DIR. DoIT shall not release any data directly to outside agencies.

4.2.9 The special access granted to the Office of Institutional Research and the Division of Information Technology, as described above, shall not provide those offices with the ability to modify or update any University Electronic Data. However, either office may participate in the normal delegation of management of subsets of University Electronic Data, and may update access to those delegated sets of data under the normal process as described in this policy.

4.3 Separation of duties

4.3.1 To the extent possible, Data Stewards or Data Managers shall authorize access to University Electronic Data in such a manner as to ensure an appropriate separation of duties. This separation of duties should ensure that no individual could enter invalid data, modify existing data, or produce erroneous records or reports in order to hide or obscure inappropriate activity.

4.4 Accuracy and integrity of University Electronic Data

4.4.1 Data Stewards shall be responsible for the accuracy and integrity of the data under their purview. Data Stewards shall collectively define standards for the entry and coding of University Electronic Data in shared environments. The CDS shall have the authority to approve these standards and resolve any conflicts about their definition.

4.5 Audit and review of University Electronic Data

4.5.1 The CDS or the Office of Internal Audit shall have the authority to audit the access authorized and actually granted to Data Users, and the accuracy and integrity of University Electronic Data, at any time. Other offices may be enlisted to assist in an audit.

4.5.2 The appropriate Data Steward or Data Manager shall review all access to University Electronic Data under his or her purview at least annually. This periodic review will include ensuring that access of Data Users is limited to that required by their duties and that separation of duties is maintained. In the event that legal requirements, job duties of Data Users or other factors have changed, the Data Steward or Data Manager shall adjust the access as necessary. The Data Steward or Data Manager shall document the results of the review and any actions taken. Said documentation shall be maintained and available for review.

5. RESPONSIBILITIES

5.1 Chief Data Steward

5.1.1 The CDS shall oversee the management of and access to University Electronic Data and shall develop procedures necessary to complete this task.

5.1.2 The CDS may approve standards for coding and entry of data in shared environments and shall resolve any conflicts about these standards.

5.1.3 The CDS may audit the access authorized and actually granted to Data Users as well as the accuracy and integrity of University Electronic Data as necessary.

5.2 Data Stewards

5.2.1 A Data Steward shall maintain knowledge of the University Electronic Data assigned to his or her purview, and the manner in which it is used, including any federal or state legislation governing the use of this data.

5.2.2 A Data Steward shall be responsible for the accuracy and integrity of the University Electronic Data assigned to him or her, and shall develop procedures to ensure that data is entered correctly.

5.2.3 Data Stewards shall collectively develop standards for the coding and entry of data in shared environments.

5.2.4 A Data Steward shall review the access granted to University Electronic Data under his or her purview and make adjustments as needed. Such a review must occur at least annually.

5.3 Data Managers

5.3.1 Data Managers shall fulfill any of the duties and responsibilities delegated by a Data Steward. This delegation shall not release the Data Steward from these responsibilities. Data Managers shall not further delegate these duties or responsibilities.

5.4 Data Users

5.4.1 Data Users shall observe all applicable federal and state legislation and university policies when accessing University Electronic Data.

5.4.2 Data Users shall review and follow any documents related to information management and security, including policies, procedures and best practices, as it is made available.

5.5 Director of Institutional Research

5.5.1 The DIR shall approve access to University Electronic Data for the staff of the Office of Institutional Research.

5.5.2 The DIR shall approve the preparation of reports or release of data by the Office of Institutional Research. The DIR shall coordinate these actions with the appropriate Data Stewards or Data Managers.

5.5.3 The DIR shall ensure that the Office of Institutional Research staff observes all legislative and policy restrictions or requirements as identified by the Data Stewards.

5.6 Chief Information Officer

5.6.1 The Chief Information Officer (CIO) shall approve access to University Electronic Data for the staff of the Division of Information Technology.

5.6.2 The CIO shall ensure that the DoIT staff observes all legislative and policy restrictions or requirements as identified by the Data Stewards.

5.7 Office of Internal Audit

5.7.1 The Office of Internal Audit may query data in order to verify its accuracy.

5.7.2 The Office of Internal Audit shall audit the access authorized and actually granted to Data Users as necessary.

6. RANGE OF DISCIPLINARY SANCTIONS

6.1 Persons in violation of this policy are subject to a full range of sanctions, including, but not limited to, disciplinary action or dismissal from The University of North Carolina at Pembroke. Any sanctions against employees will be imposed through procedures consistent with any applicable state, UNC General Administration, and federal regulations. Some violations may constitute criminal or civil offenses, as defined by local, state and federal laws, and the university may prosecute any such violations to the full extent of the law.