CONTENTS

1. PURPOSE

This document outlines the information types used by the University of North Carolina System Office (UNC-System Office), classifies information into levels of sensitivity, establishes requirements and ownership for securing each category, clarifies storage, use and accessibility requirements and explains consequences for failure to comply.

2. DATA CATEGORIES AND OWNERSHIP

Security measures for information are set by the defined roles below.

Data Owner – UNC-System Office senior administrators who have planning and policy-level responsibility for information within their functional areas and management responsibilities for defined segments of institutional information. Responsibilities include assigning Data Stewards, participating in the establishment of policies, advocacy regarding management tools and promoting data resource management for the good of the entire University.

Data Steward – UNC-System Office administrators (designated by Data Owners) who have direct operational-level responsibility for information management. Data Stewards are the managers of information/data. Data Stewards classify information as restricted or otherwise, determine how the information can be accessed, assign access privileges, and manage retention and disposal. Data Stewards work with Data Owners to develop and implement policies and procedures for requesting, maintaining and when appropriate removing access to information.

Data User – Data Users are individuals who need and use University data as part of their assigned duties or in furtherance of assigned roles or functions within the University community. Individuals who are given access to sensitive information are in a position of special trust and as such are responsible for protecting the security, integrity and privacy of that information. Some Data Users may also be Data Stewards and/or Data Owners or hold other roles identified in this document.

The Department of Information Technology (DoIT) at the UNC-System Office has primary responsibility for implementing systems to help ensure the confidentiality, integrity, availability, backup, and recovery of UNC-System Office email and electronic files saved on UNC-System Office supported storage locations. However, all Data Owners, Data Stewards, and Data Users are also separately responsible as individuals for protecting the information resources of the UNC System. Data Owners and Data Stewards are primarily responsible for ensuring the appropriate physical protections for hard copy or paper information classified above level 1 as well as for electronic information other than UNC-System Office email and shared UNC System Office supported data storage locations, and should work with IT so that appropriate protections can be established for any such data. Data Users are primarily responsible for ensuring the protection of UNC-System Office information saved on personal devices and System Office-issued devices.

The table below on pages 5-6 outlines the high-level categories of data used within the UNC-System Office and identifies the Data Owner and Data Steward responsible for ensuring the security of that data. The Senior Vice President of the division who is primarily responsible for the use of any information not currently listed in the table is the Data Owner for that data and should designate the Data Steward for that data. Data Owners or their delegates are responsible for notifying the Chief Information Security Officer (CISO) if any of the designations in the table on pages 5-6 below change or if additional categories of information should be included in that table.

3. DATA CLASSIFICATION AND SENSITIVITY LEVELS

Whether data is downloaded from a system or application within UNC-System Office's protected infrastructure or acquired by some other means, all users must secure and protect the information according to the level of its classification. The following table on page 3 below is provided to UNC-System Office Data Owners, Data Stewards, and Data Users to help them make decisions about appropriate information handling based on classification level.

Please note that the examples in the chart below are not an exhaustive list of the types of information used, created, or stored by the UNC-System Office. Data Stewards and Data Users should use their professional judgment in making decisions about how to classify information not included in the examples below, and should contact the Division of Legal Affairs or DoIT for assistance. Information belonging to multiple classification levels must be treated according to the highest level of sensitivity.

Data Classification Level		Examples	Secure Storage & File Exchange
Confidential Data Level 3 High Security	Data that, if disclosed without authorization, could reasonably result in significant financial losses, the violation of state or federal law or regulation or unacceptable risks.	Student sensitive information (whether created at UNC-System Office or received from one of the constituent institutions) that is protected by the Federal Education Rights and Privacy Act (FERPA) such as disciplinary records. The following in combination with name: • Authentication information: biometric information, passwords, digital signatures • Social Security Numbers • Passport or national identifiers • Tax ID numbers • And others specified in the NC ID Theft Protection Act	Approved Storage: This information may be stored only in UNC System Office-provided or sponsored file server space labeled "secure," or, where appropriate, in designated, enterprise databases. Secure Exchange: This data may be exchanged only using DoIT-approved methods, including https or SFTP encrypted services and ShareFile.
Enterprise Data Level 2 Medium Security	Proprietary information produced for business use by University affiliates with a legitimate business purpose to access such data.	• Internal policies, procedures, and memorandums that are intended for limited distribution • Budget and salary or other personnel information that is not designated as public by North Carolina law • Attorney-client privileged information • Audit-related information protected from public disclosure by applicable law • University emails	This data may be stored in University provided network space, ShareFile or Google Drive storage with restricted access controls. It may be shared via all University-owned, maintained, or purchased devices, solutions, and services.
Public Data Level 1 Minimum Security	Institutional information that has few restrictions and/or is intended for public use	• Directory information • Press releases • Job postings • Training designed for public consumption • Catalogs and bulletins	No restrictions for public data. This data can be stored and shared without restriction.
Personal Data Level 0	Data created or stored by individual University employees that is not connected to University business.	• Personal emails • Personal documents, such as individual tax returns, personal correspondence not connected to University business, etc.	This data should not be created or stored on University-owned, maintained, or purchased devices, solutions, or services.

Examples of data handling by classification level:

SERVICE	0	1	2	3	COMMENTS
UNC-System Office Owned Workstations, Laptops, Tablets, other devices		✓	✓		No level 0 or 3 data may be stored here. Mobile devices must have additional security configurations (e.g. passcode protection) in place if storing level 2 data.
Publicly Accessible Kiosks and Workstations		✓			No level 0, 2, or 3 data may be stored here.
Personally Owned Workstations, Laptops, Tablets, other devices	✓	✓	✓		No level 3 data may be stored here; access to any level 2 data should be done through a secure (encrypted) access protocol.
IT-Provided Non-Secured Network Drives (H:\, etc.)		✓	✓		No level 3 data may be stored here. Level 2 data should be stored here only if additional security is in place such as limited access and/or encryption
IT-Provided Secure Network Drives		✓	✓	✓	This is the preferred storage location for Level 3 data that is not directly confined to a secured database environment.
ShareFile Drive		✓	✓	✓	This is the preferred storage location for Level 3 data that must be shared with outside entities for temporary periods of time (90 days or less).
UNC-System Office Email		✓	✓		Level 3 information via email is prohibited. Level 2 data is permissible if designated email recipients are authorized to view the information by the relevant Data Steward.
UNC-System Office Google Drive		✓	✓		No level 3 data may be stored here. Level 2 data may be stored here only if additional security is in place such as limited access.
Public Cloud Storage Sites (e.g., Box)					No UNC System Office data may be stored here unless such storage is specifically approved by the CIO or CISO AND the relevant Data Owner or Steward in written form.
Public UNC-System Office websites (including Drupal offering, departmental websites, WIKIs, etc.)		✓			No level 0, 2 or 3 data may be stored here.
Secured UNC-System Office websites (Student Data Mart, etc.)		✓	✓	✓	Access to secured websites must be reviewed as defined in the User Identity and Access Control standard. .
Secured Insight Analytics Dashboards and Data Sources		✓	✓	✓	Both user access controls and network access controls must be in place and maintained to protect unit record data.
Active Collab		✓	✓		No level 0 or 3 data may be stored here.
Portable Electronic Storage Media, such as USB devices, CD/DVD, or external hard drives.		✓	✓		No level 0 or 3 data may be stored here. Portable storage media must have additional security configurations in place if storing level 2 data.

4. DATA RETENTION AND DISPOSITION

Data Owners are responsible for communicating retention and disposal policies and procedures, established in consultation with the Division of Legal Affairs and IT and consistent with the University General Records Retention and Disposition Schedule, which governs the retention, destruction, transfer, or disposal of records by the University and is accessible here: http://www.northcarolina.edu/?q=legal-affairs/records-retention.

When disposing of data, use UNC System Office-approved software and methods, as described here: http://help.northcarolina.edu or create help ticket via help@northcarolina.edu.

5. EMPLOYEE PROTECTIONS AND STAFF DEBRIEFINGS

UNC-System Office takes the security of its data extremely seriously. Employees who fail to comply with these procedures may be subject to formal disciplinary action, up to and including dismissal. It is the responsibility of each individual employee to read, understand, and adhere to these procedures. Any UNC-System Office employee who believes that an office, division, or organizational policy or practice is not in compliance is encouraged to contact his or her supervisor, the Chief Information Security Officer or Internal Audit to discuss those concerns.

6. DATA OWNERS AND STEWARDS

Category	Owner	Steward(s)
Advancement Data	Vice President for Advancement	Director of Gift Planning
Board of Governors Materials	Sr. Associate Vice President and University Secretary	Associate Secretary
President's Office Information and Materials	Chief of Staff	Chief of Staff or designee
Finance and Budget Data	Sr. Vice President for Finance and Budget	Vice President for Financial Planning & Analysis For internal accounting data, Controller For purchasing data, Director of Purchasing For capital planning data, Associate Vice President for Capital Planning
HR Data (includes position data, employee data, benefits data, UNC System Office payroll data, employee eligibility data, grievance data, timecard data, and background check information, etc.)	Vice President for Human Resources	Senior Associate Vice President for Human Resource Services For shared services payroll data, Director of Payroll Shared Services

IT Account and Log Data	Vice President for Information Technology and Chief Information Officer	Director of Infrastructure and Operations
Legal Information (includes attorney-client privileged information, work product, contracts, policies, complaints, investigations, public records, presentations, etc.)	Sr. Vice President and General Counsel	Vice President for Legal Affairs and Deputy General Counsel
Research Data (including grants and awards)	Sr. Vice President for Academic Affairs	Director of Sponsored Programs
Institutional Student Data (includes admissions data, registration data, grade data, course data, financial aid data, etc.)	Vice President, Data and Analytics	Associate Vice President for Data & Analytics
Academic Affairs Operational Program Data	Sr. Vice President for Academic Affairs	Vice Presidents of the applicable programs and areas of responsibility
Strategic Planning, Initiatives and Policy Data	Sr. Vice President for Strategy & Policy	For strategic planning and initiatives, Vice President of Strategic Initiatives For policy, analysis, program data, Associate Vice President for Planning & Analysis
Government Relations and External Affairs Data	Sr. Vice President for External Affairs	s Vice Presidents of the applicable programs and areas of responsibility
Communications Data	Vice President, Communications	Assistant Vice President for Strategic Relations For media relations data, Associate Vice President for Media Relations
Academic/University K12 Data	Sr. Vice President for Academic Affairs	Vice President of Academic & University K12 Programs
Audit and Compliance Data	Sr. Vice President and General Counsel	Vice President for Compliance & Audit Services
Safety and Emergency Operations Data	Sr. Vice President and General Counsel	Associate Vice President for Safety & Emergency Operations

Write help@northcarolina.edu for clarification and/or to request exceptions.

Revisions of the above will be communicated as soon as practicable to all UNC-System Office employees.

END OF DOCUMENT