
OFFICE OF THE CHANCELLOR
University of New Orleans

Administrative Policy & Procedure

AP 28.01

Revised 07/01/2009

Supersedes AP 28.01, dated 01/23/2009

SUBJECT: Data Classification and Data Security

PURPOSE: To provide a systematic method to ensure all University Data is properly categorized and classified by the appropriate Functional Unit; and to ensure that all users are made aware of Data security issues.

AUTHORITY: *Article VII, Section 4, By-Laws and Regulations of the Board of Supervisors of the Louisiana State University System.*

OBJECTIVE: To establish a process of categorizing and classifying Data in order to further address Data security responsibilities and concerns.

DEFINITIONS

1. Access to Data - an additional level of Data protection controlled at the user level, to limit, restrict, and monitor access to Data records.
2. Authorized Use - guards against use of The University of New Orleans systems and infrastructure for malicious acts against its own systems as well as attacks against other individuals and organizations.
3. Availability of Data - ensures timely and reliable access to and use of Data and information technology resources to carry on the mission of the University. These resources include assets such as intellectual property, research and instructional Data and systems, and physical assets.
4. Computing Resources - all devices (including, but not limited to, personal computers and laptops) owned by the University, the user or otherwise, which are part of or are used to access a) the University network, peripherals, and related equipment and software; b) Data/voice communications infrastructure, peripherals, and related equipment and software; c) and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by University Computing and Communications (UCC) resources or components thereof may be individually assigned or shared, single-user or multi-user, stand-alone or networked, and/or mobile or stationary.
5. Confidential Information- Data that by law is not to be publicly disclosed. This designation is used for highly sensitive information whose access is restricted to authorized employees. Confidentiality provides protection of information from either intentional or accidental attempts to access personal or University information by unauthorized entities. Confidentiality covers Data in storage, during processing, and in transit. State and federal laws and regulations require the University to take reasonable steps to ensure security of some classifications of Data (e.g., FERPA, HIPAA).
6. Data - all information that is used by or belongs to the University, or that is processed, stored, maintained, transmitted, copied on, or copied from University computing resources.

7. Data Steward – designated personnel within Functional Units that are responsible for the collection, maintenance, and integrity of the Data for that specific area.
8. Functional Unit- any campus, college, program, service, department, office, operating division, vendor, facility user, or other person, entity or defined unit of The University of New Orleans that has been authorized to access or use computing resources or Data.
9. Individual User - any person or entity that utilizes computing resources, including, but not limited to, employees (faculty, staff, and student workers), students, agents, vendors, consultants, contractors, or sub-contractors of the University.
10. Integrity of Data - protection against either intentional or accidental attempts by unauthorized entities to alter Data or modify information systems to impede it from performing its intended function. Integrity requires maintaining the University's reputation to manage the resources entrusted to it.
11. Least Privilege Principle - the principle that requires each person and/or Functional Unit to be granted the most restrictive set of privileges needed for the performance of authorized tasks.
12. Mission Critical Data- Public, Private or Confidential Data identified by the Data Steward as vital to the mission of the University. Unless otherwise authorized by the appropriate Data Steward, Mission Critical Data must be backed up on centralized servers maintained by the University.
13. Private (Internal) Data - any internal Data that derives its value from not being publicly disclosed, which includes information that the University is under legal or contractual obligation to protect.
14. Protected Information - Data that has been designated as Private or Confidential by law or by the University. Protected information includes, but is not limited to, employment records, medical records, student records, education records, personal financial records (or other personally identifiable information), research Data, trade secrets, and classified government information. Protected information shall not include public records that by law must be made available to the general public. To the extent there is any uncertainty as to whether any Data constitutes protected information, the Data in question shall be treated as protected information until a determination is made by the University or proper legal authority.
15. Public Data - Data that any person or entity either internal or external to the University can access.

GENERAL POLICY

This policy establishes procedures for the categorization and classification of Data, sets forth methods for securing Data, and delineates the responsibilities of all Individual Users with respect to the maintenance of Data security.

PROCEDURE

The process of developing and implementing will be conducted in the following three phases; **PHASE I** Appointment of Data Stewards within Functional Units; **PHASE II** Classification of Data; **PHASE III** Recording of Data Classifications; and **PHASE IV** Continuing Review. The University's Records Management Committee will oversee the entire process.

PHASE I

APPOINTMENT OF DATA STEWARD

The Chancellor shall appoint a Data Steward for each Functional Unit to ensure that the University meets external and internal requirements for privacy and security of specific types of confidential and business information (e.g., student records, employee records, health records, financial transactions). This information should be communicated to either the Records Management Officer or the University's Records Management Committee recordscommittee@uno.edu.

MAIN DATA TYPES AND RESPONSIBLE FUNCTIONAL UNIT. For purposes of this policy, Data is divided into categories, and the Functional Unit responsible for the Data is noted:

- Accreditation, Institutional Statistics, and Academic Program Records (Academic Affairs)
- Computing and Network Infrastructure Records (UCC)
- Employment Records, Including Benefits (HRM)
- Facility Operations Records (Campus Services)
- Financial Records (Financial Services)
- Intellectual Property Records (Technology Transfer)
- Law Enforcement Records (UNO Police)
- Legal Records (University Counsel)
- Library Records (Earl Long Library)
- Policy and Regulatory Compliance, including NCAA records (Office of the Chancellor)
- Research and Sponsored Programs Records (Office of Research & Sponsored Programs)
- Student Academic Records (Registrar)
- Student Financial Aid Records (Student Financial Aid)
- Student Health Records/ Disability Services Records (Student Affairs)
- Student Judicial Records (Student Affairs)

PHASE II

CLASSIFICATION OF DATA

Data Stewards are advised to seek direction from the appropriate University administrative units, University Counsel, and the Records Management Officer to ensure accuracy and completeness throughout the classification of data process.

- A. CATEGORIZING AND CLASSIFYING DATA.** All Data, whether in hardcopy or electronic form shall be classified according to the categories outlined in **Table 1**. Data categories are as follows:
- i. PUBLIC DATA.** The disclosure, use, or destruction of Public Data should have no adverse affects on the University nor carry any liability. Examples of Public Data include readily available news and information posted on the University's website.
 - ii. PRIVATE DATA.** Internal Data that would lose its value to the University and/or the custodian of such Data would be destroyed or diminished if such Data were improperly disclosed to others. Private Data may be copied and distributed within the University only to authorized users. Private Data disclosed to authorized, external users must be done in accord with a non-disclosure agreement. Examples of Private Data include employment-related Data.
 - iii. CONFIDENTIAL DATA.** Confidential Data may be disclosed only if the individual to whom such Data is to be disclosed has a valid need for access and the

disclosure is specifically authorized by the appropriate Data Steward or designee. Confidential Data may not be copied without authorization from the identified custodian and will not be disclosed except as provided by University policy and procedures, or as required by operation of law or court order. Examples of Confidential Data include, but are not limited to, personally identifiable information in student education records, and personally identifiable non-public information about University employees.

NOTE: Anyone creating a new information system that will store or handle Confidential Data must inform either the Records Management Officer or the Records Management Committee recordscommittee@uno.edu.

TABLE 1			
GENERAL GUIDE FOR CLASSIFICATION OF DATA			
	CONFIDENTIAL DATA	PRIVATE DATA	PUBLIC DATA
LEVEL OF SENSITIVITY	Highest, Most Sensitive	Moderate Level of Sensitivity	Low Level of Sensitivity
ACCESS RESTRICTIONS	Only those individuals designated with approved access, signed non-disclosure agreements, and a need-to-know	UNO employees and non-employees who have a business need-to-know	UNO affiliates and general public with a need-to-know
LEGAL REQUIREMENTS	Protection of Data is required by law (e.g., HIPAA, FERPA)	UNO has a contractual obligation to protect the Data	Protection of Data is at the discretion of the owner/custodian
REPUTATION RISK	High	Medium	Low
OTHER INSTITUTIONAL RISKS	Information which provides access to resources, physical or virtual	Smaller subsets of protected Data from a school or department	General University information
EXAMPLES	<ul style="list-style-type: none"> • Student records and unique student identification numbers • Prospective students • Employment Records¹ • Health records and information • Human subjects research Data that identifies individuals • Financial transactions of students and employees • Personally Identifiable Financial Information 	<ul style="list-style-type: none"> • Information resources with access to confidential Data • Research Data or results that are not confidential Data • Information covered by non-disclosure agreements • Materials for performance of official duties • Proprietary information of UNO or others contained within proposals, contracts, or license agreements 	<ul style="list-style-type: none"> • Campus maps • Personal directory information (e.g., contact information) • Departmental websites • Academic course descriptions • News • Information posted on University website • Budgets • Purchase Orders

¹ Although certain records contained within employment files may be “public records” subject to disclosure under Louisiana State Revised Statute 44:1, such records should be maintained as Confidential Data and disclosure of “public records” shall only be made after a case-by-case determination.

- B. TREATMENT OF ELECTRONIC DATA.** For the purpose of this policy, electronic mail (e-mail) and electronic files stored on University servers should be classified by the Data or information contained therein. For example, e-mails that relate to specifically identified students must be kept as confidential education records. Each user should protect their e-mails and electronic files in accordance to [UNO Information Technology General User Policies](#).
- C. TREATMENT OF INTERMINGLED DATA.** Often public records are intermingled with confidential Data and protected information, in such cases all the information and Data should be protected as confidential until it is necessary to segregate any public records.

PHASE III

RECORDING OF DATA CLASSIFICATION

Phase II classification of Data will be used to complete the Functional Unit's Records Retention Schedule throughout Phase III. Upon review and approval by the University's Records Management Committee, the Records Management Officer will submit the Records Retention Schedule to the Louisiana Secretary of State, Division of Archives, Records Management and History for agency approval.

SECURITY OF DATA

Data Security and Access to Data will be determined in accordance with Phase II Data Classifications.

- A. DATA ACCESS.** Access to Data will be authorized in accordance with the principle of Least Privilege, the application of which is intended to reduce the risk of harm that may result from accidental disclosure or unauthorized use of Private or Confidential Data. Access to Data may be further restricted by law, beyond the classification systems of the University. Access to Confidential Data is allowed only with the written or verbal approval of the responsible Data Steward or designee. Access rights must be reevaluated upon separation from employment or when an employee's job duties change.
- B. MISSION CRITICAL DATA.** There are additional security concerns related to Mission Critical Data. Such Data can be found in any Data category: Public, Private, or Confidential. Mission Critical Data shall be determined by the Data Steward of each Functional Unit. In addition, the Data Steward must notify University Computing and Communications (UCC) of the specific Data classified as Mission Critical Data in order for that data to be backed up on centralized servers maintained by the University.
- C. EXTERNAL REQUESTS FOR DATA.**
- i. **Confidential Data** shall not be provided to external parties or users without approval from the Data Steward (e.g., Mortgage Verification, Garnishments, etc). In cases where the Data Steward is not available, approval may be obtained by the Director or Department Head of the office in which the Data is maintained, or by an official request from a senior executive officer of the University (e.g., Chancellor, Executive Vice Chancellor/Provost, or Vice Chancellor).
 - ii. **Public Information Requests.** Subject to statutory exceptions, *Public Records* are available for inspection and/or reproduction through the Office of the University Counsel, in accordance to the Louisiana Public Records Act (La.

R.S. 44:1, *et seq*) and Article XII, Section 3 of the Louisiana Constitution. For details, please refer to [AP 28.03 Public Information Requests](#).

D. REPORTING OF SECURITY INCIDENTS. Reporting security breaches or other security-related incidents is an ethical responsibility of all members of The University of New Orleans community. Security breaches must be addressed promptly and with the appropriate level of action. [UNO IT User Policy](#) outlines the responsibilities of colleges, departments, units, and individuals in reporting as well as defining procedures for handling security incidents.

E. DATA SECURITY POLICIES. University Computing and Communications (UCC) has overall responsibility for the data security of the University's information technologies. Implementation of data security policies is delegated throughout the University to various University services, such as colleges, departments, and other units; and to individual users of campus information technology resources. Refer to [UNO IT User Policy](#) for details.

PHASE IV

CONTINUING REVIEW

Review and revision of the Data Classification and Data Security process will be conducted during Phase IV as needed in accordance with the schedule established by the Louisiana State Archives.

RESPONSIBILITIES

Colleges/Departments are responsible for securing any information they create, manage, or store, and for any information they acquire or access from other University systems (e.g., student records, employment records, business information).

Data Stewards are responsible for general record security issues and for ensuring compliance to LSU System and University policies, as well as standards and best practices in the areas of their responsibility. Data Stewards are responsible for advising colleges, departments, units, and individuals within their functional area in Data classification and Data security practices. It shall be the responsibility of the Data Steward(s) to classify the Data, with input from appropriate University administrative units and legal counsel. The Data Steward(s) are responsible for communicating the level of classification to individuals granted access.

Functional Units are responsible for managing and maintaining the security of the Data, computing resources and protected information. Functional Units are responsible for implementing appropriate managerial, operations, physical, and technical controls for access to, use of, transmission of, and disposal of Data in compliance with this policy.

Individual Users are responsible for protecting the security of University information and information systems by adhering to the objectives and requirements stated within published University policies. In addition, individuals are required to comply with the additional security policies, procedures, and practices established by colleges, departments or other units. Failure to comply with established policies and practices may result in loss of computing privileges and/or disciplinary action. Students, faculty, and staff who use

personally-owned systems to access University resources are responsible for the security of their personally-owned computers or other network devices and are subject to [UNO IT User Policy](#) and all other laws, regulations, or policies directed at the individual user.

University Computing and Communications (UCC) has overall responsibility for security of the University's information technologies and implementation of Data security policies.

Timothy P. Ryan
Chancellor