THE UNIVERSITY of NEW ORLEANS	**Policy No:**	**AP-AA-17.3**
	TITLE:	**Data Classification and Data Security**
	EFFECTIVE DATE:	**August 8, 2005*** **(*Policy Revised, see below)**
	CANCELLATION:	
ADMINISTERED BY: Office of the Provost and Senior Vice President for Academic Affairs	**REVIEW DATE:**	**Spring 2020**

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

LA R.S. 44:1, et seq., LA R.S. 44:412; Part Two, Chapter III, Section IV of the Bylaws and Rules of the University of Louisiana System. University of Louisiana System Policy and Procedure Memorandum M-17 (Records Retention and Litigation Hold).

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 - refers to a user's ability to access or retrieve data stored within a database or other repository. Data protection may limit user's access to certain controlled, confidential, or other data.

2. Data and Information- There is a subtle difference between data and information. Data are the facts or details from which information is derived. For data to become information, data needs to be put into context. For example, each student's test score is one piece of data and the average score of a class or of the entire school is information that can be derived from the given data. However, for the purpose of this document, we mainly use the term data to also include information that is derived for the data.

3. Authorized Use **-** faculty, staff, students, or other University affiliated person who has been granted access to **t**he University of New Orleans data systems. There are many levels of authorization, depending on the type and nature of the user's responsibilities.

   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, servers, desktop and laptop computers, portable scanners, PDAs owned by the University, databases (web enabled or otherwise) and any other systems in direct or indirect support of information systems and all other associated tools, instruments, facilities, and the services that make use of any technology resources owned, operated, or controlled by the university. Computing resources are used for access to 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. Private/Protected/Confidential Information- data that by law is not to be publicly disclosed. In terms of public disclosure and safeguard, "Private", "Protected" and "Confidential" data are treated the same. Herein, the term "Confidential" would apply to "Private" and "Protected" data as well. The designation is used for highly sensitive data whose access is restricted to authorized employees. Confidentiality provides protection of data 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. Confidential information includes, but is not limited to, employment records, medical records, mental health records, student records, education records, personal financial records (or other personally identifiable information), research data, trade secrets, and classified government information. Confidential data 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 Confidential data, the Data in question shall be treated as confidential data until a determination is made by the University or proper legal authority. Data may be released if pertinent release forms are sign (FERPA release, transcript authorization, etc.)

6. University 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, protection 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 - maintenance and the assurance of the accuracy and consistency of data over its entire life-cycle. Data integrity is essential to smooth operation of the university. Therefore, 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 is an essential part of the data integrity process.

11. Least Privilege Principle - limiting access to the minimal level that still allows normal performance of duties. 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 that is essential to the operation of the university. Failure or disruption to mission critical data will result in serious impact on the operation of the campus in particular on its vital mission of teaching. Mission critical data must be backed up on centralized servers maintained by the University.

13. 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 Information Technology Advisory Council will oversee the entire process.

PHASE I - APPOINTMENT OF DATA STEWARD

The head of each Functional Unit (e.g., Registrar) is designated as the Principal Data Steward for each Functional Unit with the responsibility of ensuring 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 the Information Technology Advisory Committee (ITAC).

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, and Academic Program Records (Academic Deans)
- Institutional Statistics (Office of Institutional Research and Effectiveness**)**
- Computing and Network Infrastructure Records (Information Technology)
- Employment Records, Including Benefits (Human Resource Management)
- Facility Operations Records (Facility Services)

- Financial Records (Business Affairs)
- Intellectual Property Records (Office of Research and Economic Development)
- Law Enforcement Records (UNO Police)
- Legal Records (University Counsel)
- Library Records (Earl K. Long Library)
- Mental Health Records, including client session video recordings (Counseling Services)
- Policy and Regulatory Compliance, including NCAA records (Office of the President)
- Research and Sponsored Programs Records (Office of Research and Economic Development)
- Student Academic Records (Registrar)
- Student Financial Aid Records (Student Financial Aid)
- Student Health Records/ Disability Services Records (Student Health Services)
- 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 effects 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 if it 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 to authorized individuals with 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, information contained in health records and mental health 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 the Information Technology Advisory Committee (ITAC).

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 nonemployees who have a need-to-know	UNO affiliates and general public
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	Extremely High	High	Low to Medium
OTHER INSTITUTIONAL RISKS	Information that could severely compromise the operation of the institution	Information that may delay or curtail general business processes	No other risks
EXAMPLES	• Student records and unique student identification numbers • Prospective students • Employment Records* • Health records and Information • Mental Health Records • Human subjects research • Data that identifies Individuals • Financial transactions	• Information resources with access to confidential Data • Research Data or results that are not confidential Data • Information covered by nondisclosure agreements • Materials for performance of official duties • Proprietary information of UNO or others contained within proposals, contracts, or license agreements	• Campus maps • Personal directory information (e.g., contact information) • Departmental websites • Academic course descriptions • News • Information posted on University website • Budgets • Purchase Orders

	of students and employees • Personally Identifiable Financial Information			

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.

TREATMENT OF ELECTRONIC DATA. For the purpose of this policy, electronic mail (e-mail) and electronic files stored on University servers (or any other devices) 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. Note: No confidential data/information may be submitted via email or stored in the public folder of the S-Drive.

TREATMENT OF INTERMINGLED DATA. Often public records are intermingled with confidential data and/or 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 Information Technology Advisory Council, 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 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 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 Information Technology of the specific Data classified as Mission Critical Data in order for that data to be properly backed up on centralized servers maintained by the University.

C. EXTERNAL REQUESTS FOR DATA.

i. **Confidential and Private Data** shall not be provided to external parties or users without written approval by an official request from a senior executive officer of the University (e.g., President, Provost and Senior VP for Academic Affairs, or Vice President for Business Affairs).

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 and by the way of this AP statutory 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 Information Technology 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 UL 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 Information Technology has overall responsibility for security of the University's information technologies and implementation of data security policies.

John W. Nicklow
President
University of New Orleans

**Policy Updates:*
Revisions: 1/3/2017