ADMINISTRATIVE POLICY

Policy Proposal Title	Data Classification Policy
Policy Subtitle/Subject	This policy establishes uniform data classification levels for University Data and identifies the shared responsibilities for classifying University Data.
Responsible Executive(s) (RE)	General Counsel Vice President, Information Technology and Chief Information Officer Chief Information Security Officer
Responsible Office(s) (RO)	Office of General Counsel ; Information Technology
Primary Point of Contact from RO	Ross Janssen
Contact Information (email and phone)	rjanssen@tulane.edu
Date Proposed	10/4/22
Reviewed	**1/10/23**
Last Updated	**1/10/23**
Effective Date	**1/10/23**

☒Permanent ☐Temporary

1.0 POLICY STATEMENT

University Data, which includes Academic, Clinical, Research, and Administrative Data, is not owned by a particular department; they are valuable assets of the University as a whole. Tulane is committed to protecting the privacy of University Data. It is our collective responsibility to safeguard and use the data to further the institutional mission, with availability of data to individuals with a legitimate need for it, consistent with the University's responsibility to preserve and protect such information.

2.0 PURPOSE AND SCOPE

All members of Tulane University have a responsibility to protect University Data from unauthorized access or disclosure. The purpose of this policy is to establish a framework for classifying University Data based on level of sensitivity, criticality, relevant compliance requirements, and the impact on individuals and the University should the data be improperly used, disclosed, altered or destroyed. The classification scheme applies to all University Data both physical and electronic and will inform the baseline security controls for protection of the data. The classification of specific University Data is subject to change based on risk assessment and as the attributes of that data change (e.g., its elements, content, uses, importance, method of transmission, or regulatory context).

3.0 APPLICABILITY OF THIS POLICY

This policy applies to all faculty, staff, students, student employees, volunteers, and contractors who have access to University Data. This policy covers data that is stored, accessed, or transmitted in all formats, including electronic, magnetic, optical, paper, or other non-digital formats. With the exception of those classes of data expressly protected by statute, contract, or industry regulation, the data classification examples presented below are guidelines.

4.0 WEBSITE ADDRESS FOR THIS POLICY

https://policy.tulane.edu/policy-library

5.0 CONTACTS

Subject	Contact	Telephone	E-mail/Web Address
Data Classification	Ross Janssen	504-988-7739	rjanssen@tulane.edu

6.0 CONTENT

1.0 POLICY STATEMENT **1**

2.0 PURPOSE AND SCOPE **2**

3.0 APPLICABILITY OF THIS POLICY **2**

4.0 WEBSITE ADDRESS FOR THIS POLICY **2**

5.0 CONTACTS **2**

6.0 CONTENT **2**

7.0 DEFINITIONS **3**

8.0 POLICY AND PROCEDURES **6**

8.1 **Data Classification Levels** 6

8.2 **Data Classification Guidelines** 8

9.0 CONSEQUENCES OF VIOLATING THE POLICY 8

APPENDIX I RELATED POLICIES, LAWS, REGULATIONS OR PROCESSES 8

7.0 DEFINITIONS

Academic Data: Academic Data is data collected in support of the academic operations of the University, inclusive of information directly related to the individual student. These would include student information such as grades, test scores, attendance, transcripts, financial aid information, and any analytical data collected about students.

Administrative Data: Administrative Data is collected in support of the administrative and business operations of the University, such as the delivery of services to University units and departments. A substantial number of functions at the University incorporate collections of Administrative Data, such as admissions, student financial aid, records/registrar, alumni/advancement, the business office, investment management office, and human resources, including data utilized in Tulane's EDI initiative.

Chief Privacy and Data Compliance Officer: The Chief Privacy and Data Compliance Officer is responsible for (i) coordinating all activities related to University Data Management, and (ii) ensuring that procedures are developed by functional offices to address those cases where a member of the University community seeks permission to access University Data beyond the normal performance of their duties. The Data Trustees will review and ratify the procedures as developed.

Clinical Data: Clinical Data are information, records, and tangible products collected during the course of patient care or as part of a formal clinical trial program. Clinical data would include electronic health records, clinical administrative data, claims data, patient/disease registries, health surveys, and clinical trials data. Clinical data is subject to all requirements documented within this policy as well as any additional requirements found within the Research Data Policy, if applicable, and/or any other clinical policies.

Data Classification: Data Classification refers to the categorization of University Data and the consistent application of security standards based on such categorization.

Data Custodians: The Data Custodians are employees with information technology expertise assigned to each Information System that maintains University Data. Data Custodians (i) oversee the safe transport and storage of data according to requirements of the appropriate classification(s), (ii) ensure data is stored only on official supported Tulane storage mechanisms and locations, (iii) establish and maintain the underlying infrastructure, and (iv) perform activities required to keep the data intact and available to users. In addition, Data Custodians are responsible for working with Data Stewards, the Chief Privacy and Data Compliance Officer, and data support groups to develop automated processes that identify

erroneous, inconsistent, or missing data. Data Custodians work with data support groups, the Chief Privacy and Data Compliance Officer, and Data Stewards to resolve data issues.

Data Governance Council: The Data Governance Council establishes overall policies for management and access to University Data. This committee shall be composed of the Data Trustees; shall be chaired by an elected member of the Data Governance Council; shall approve the policies and procedures developed in each functional area by the Data Stewards and Data Trustees to ensure appropriate compliance with this policy and applicable regulations; shall provide oversight of all University processes which capture, maintain, and report on Administrative Data; and shall approve any decisions to archive Administrative Data.

Data Handling: Data Handling refers to the actions that Data Users should take to use, process, transmit, store, archive, and destroy University Data in a secure manner that aligns with the classification of the data.

Data Lifecycle: The progression of stages in which a piece of information may exist between its original creation or collection and final archival or destruction.

Data Stewardship Advisory Group: The Data Stewardship Advisory Group is a University-wide committee, primarily composed of Data Stewards. Designated Data Users may be invited to attend, as appropriate. This group reviews the operational effectiveness of University Data management policies and procedures and makes recommendations to the Data Governance Council for improvement or change. Data Stewards will share best practices during their meetings, as well as raise concerns which cross functional areas. The group is chaired by an elected member of the group. The Data Stewardship Advisory Group must ensure regular and appropriate collaborative communication with Data Users on any operational changes which impact business processes and data.

Data Stewards: Data Stewards are typically operational managers in a functional area with day-to-day responsibilities for managing business processes and establishing the business rules for the Transactional Systems. Data Stewards will collaborate with Data Trustees to set the classification of data within their area of responsibility. Data Stewards are responsible for reviewing and maintaining the data classifications and handling procedures defined in this policy and other related policies. Data Stewards are appointed by the respective Data Trustee.

Data Trustees: Data Trustees are defined as the authorized manager of the data who have planning and policy-making responsibilities for University Data and for the establishment of operational processes to collect and record data per University business rules. The Data Trustees, as a group, are responsible for overseeing the establishment of data management policies and procedures, and for the assignment of data management accountability. Data Trustees will collaborate with Data Stewards to set the classification of data within their area of responsibility. Data Trustees are also responsible for establishing the appropriate levels of training for Data Users who access the data within the Data Trustee's unit and area of responsibility.

Data Users: Data Users are individuals who access University Data (in connection with their role at Tulane (i.e., student, faculty, staff, etc.) to perform their assigned duties. Data Users are responsible for safeguarding their access privileges, for the use of the University Data in conformity with all applicable University policies, and for securing such data. So that the proper controls are applied, it is the responsibility of each Data User to:

- Know the classification of the Data being used.
- Know the type of University Data being used.
- Follow Tulane IT policies and the appropriate regulatory and security measures (join computer to domain, encryption, etc.)
- Consult the Related Policies for further information.

Information Systems: Information Systems are all computer or electronic resources that are used in the search, access, acquisition, transmission, storage, retrieval, or dissemination of data. In addition, University technology resources are any technology or services that are owned or managed by the University, that connect to the University network, connect to another University technology or service, or store University data or information.

Office of Assessment and Institutional Research: The Office of Assessment and Institutional Research shall be responsible for working with the appropriate Data Stewards to develop definitions of commonly used terms and will define how official University metrics are calculated. Further, in the course of its work, the Office of Assessment and Institutional Research will typically discover data discrepancies and inconsistencies and will promptly report such to the appropriate Data Steward for resolution.

Research Data: Research Data are information, records, and tangible products arising from or associated with research conducted at, under the auspices of, or using the resources of the University. Research Data includes both intangibles (e.g., information and copyrighted works such as software and expressions of information) and tangibles (e.g., cell lines, biological samples collected for research purposes, synthetic compounds, organisms, and originals or copies of laboratory notebooks). Research data is subject to all requirements documented within this policy as well as any additional requirements found within the Governance and Retention of Research Data Policy.

Transactional System: A transactional system is an information processing system which divides work into individual, indivisible operations, called transactions. These transactions involve the collection, modification and retrieval of data.

University Data: University Data is any data or information, regardless of electronic or printed form or location, that is created, acquired, processed, transmitted, or stored by the University. Where appropriate, University Data may be further defined as Administrative, Academic, or Research Data to provide additional management or information security guidance.

Vice President, Information Technology and Chief Information Officer: The Vice President, Information Technology and Chief Information Officer provides technology leadership and advises the Data Governance Council and Data Stewardship Advisory Group about administrative, technical, and physical safeguards to apply to the handling, use, transmission, processing, storage, and destruction of University Data.

8.0 POLICY AND PROCEDURES

Identification and classification of University Data are essential for ensuring that the appropriate degree of protection is applied to University data. The classification of University data helps determine what baseline access and security controls are appropriate for safeguarding the data.

8.1 Data Classification Levels

The University's data is classified into four categories as described in this document:

Level 1—Public. Public data is data for which the unauthorized disclosure or unauthorized modification results in low or no risk to individuals or the University. Generally speaking, Public data may be shared with a broad audience both within and outside the University community and no steps need to be taken to prevent its distribution. Normal security controls are used to safeguard Public data.

Examples of Public data include: press releases, directory information (not subject to a Family Educational Rights and Privacy Act [FERPA] exception), course catalogs, application and request forms, and other general information that is openly shared. The type of information a department might post on its website is a good example of Public data.

Level 2—Internal. Internal data is data for which the unauthorized disclosure or unauthorized modification would cause some adverse impact to individuals or the university (e.g., financial loss, reputation impact, impairment of the ability to conduct business, or violation of federal or state laws, or contractual agreements, or government regulation). Internal data generally should not be disclosed outside of the University without the permission of the Data Steward. Moderate security controls are used to safeguard Internal data.

Examples of Internal data include: Some memos, correspondence, and meeting minutes not subject to compliance or legal restrictions, ie Grand Rounds; contact lists that contain information that is not publicly available; and procedural documentation that should remain private.

Level 3—Confidential Data. Confidential data is data for which the unauthorized disclosure or unauthorized modification would cause a significant adverse impact on individuals or the university (e.g., financial loss, reputation impact, impairment of the ability to conduct business, or violation of federal or state laws, or contractual agreements, or government regulation). This classification also includes data that is required to be kept confidential by law (e.g. FERPA) or pursuant to a written confidentiality agreement such as with a vendor. High security controls are used to safeguard Confidential data.

Examples of Confidential data include:

- Student record information covered by the Family Educational Rights and Privacy Act (FERPA), excluding directory information.
- Personally identifiable information entrusted to the University that is not otherwise categorized as Restricted data, such as information regarding applicants, alumni, donors, potential donors, or parents of current or former students, and information covered by the European Union's General Data Protection Regulation (GDPR).
- The Tulane University ID Number, when stored with other identifiable information such as name or e-mail address.
- Individual employment information, including salary, benefits, and performance appraisals for current, former, and prospective employees.
- Legally privileged information.
- Information that is the subject of a confidentiality agreement.
- Human subject research data with identifiers limited to dates, city, Zip Code; such as information that is the subject of a HIPAA Limited Data Set covered by a Data Use Agreement.
- Controlled Unclassified Information required to be compliant with NIST Special Publication 800.171.

Level 4—Restricted. Restricted data is data for which the unauthorized disclosure or unauthorized modification would cause a severe adverse impact on individuals or the university (e.g., financial loss, reputation impact, impairment of the ability to conduct business, or violation of federal or state laws, or contractual agreements, or government regulation).This includes information the university has a contractual, legal or regulatory obligation to safeguard in the most stringent manner. In some cases, disclosure or loss of this data would require the University to notify affected individuals and state or federal authorities. Maximum security controls are used to safeguard Restricted data.

Examples of Restricted data include:

- Personally Identifiable Information (PII), including an individual's name plus the individual's Social Security Number, driver's license number, or a financial account number.
- Protected Health Information (PHI) subject to the Health Insurance Portability and Accountability Act (HIPAA). See the University's HIPAA Privacy Policies and Procedures for details.
- Personally identifiable health information that is not subject to HIPAA but used in research, such as Human Subjects Data.
- Financial account numbers covered by the Payment Card Industry Data Security Standard (PCI-DSS), which controls how credit card information is accepted, used, and stored.
- Data controlled by U.S. Export Control Law such as the International Traffic in Arms Regulations (ITAR) or Export Administration Regulations (EAR). ITAR and EAR have additional requirements. See the Export Controls site for details.
- U.S. Government Classified Data.
- Unencrypted data used to authenticate or authorize individuals to use electronic resources, such as passwords, keys, and other electronic tokens.

- "Criminal Background Data" that might be collected as part of an application form or a background check.
- Information covered by the Gramm-Leach-Bliley Act (GLBA), which requires the protection of certain financial records.

8.2 Data Classification Guidelines

- All university data will be classified and periodically reviewed by Data Trustees, Data Stewards and the Data Governance Council according to its use, sensitivity, and importance to the university, and in compliance with federal and/or state laws, other regulations, and contractual terms.
- Any data element or information that is not classified will be assumed to be of the Restricted level classification until otherwise determined unless the data is known to be addressed by applicable law or statute.
- How printed or electronically stored information is classified is based on the category of data contained in the document or electronic storage media or service. Information should be classified according to the highest level of data contained in the document or on the electronic storage media or service. Therefore, a document containing both Restricted and Confidential level data should be considered to be of the Restricted classification and handled accordingly.

9.0 CONSEQUENCE OF VIOLATING THE POLICY

Violation of this policy may result in disciplinary action, up to and including termination.

Failure to comply with the data classification standards outlined here and in related policies may result in harm to individuals, organizations, or the University. Violations of this policy or any law related to the use of University Data, including, but not limited to the Family Educational Rights and Privacy Act of 1974 (FERPA), the Health Insurance Portability and Accountability Act of 1996 (HIPAA), and the Gramm Leach Bliley Act (GLBA), may result in penalties and disciplinary action under rules established by Tulane University.

APPENDIX 1

RELATED POLICIES, LAWS, REGULATIONS OR PROCESSES

Information System Risk Criticality Classification Policy - *currently in draft form*

Data Management Policy

Data and System Security Policy – *currently in draft form*

Governance and Retention of Research Data – *currently in draft form*

All Tulane IT policies are here - https://it.tulane.edu/policies-guidelines-and-recommendations

Data Governance Related Laws and Regulations – Included as Attached

Tulane Data Governance Applicable Laws and Regulations

Related laws and regulations include:

• The Family Educational Rights and Privacy Act of 1974 (FERPA) was enacted, among other purposes, to protect the privacy of students' education records. The "education records" are defined as those records, files, documents, and other materials that contain information directly related to a student and that are maintained by the University or by a third party acting for the university. The form in which the information is maintained by the University does not matter. For example, computerized or electronic files, audio or videotape, photographic images, and film, with such information are "education records". This includes communications and documents distributed or received by email, or other similar University systems, which are retained in these systems, either by the sending or receiving party. See the University's FERPA-related resources for additional guidance: https://registrar.tulane.edu/privacy-policies-forms

• The Gramm-Leach-Bliley Act (GLBA), short-form for the Financial Modernization Act of 1999, was enacted to promote financial integration and develop a regulatory framework for financial institutions which deal with non-public financial information, such as financial aid, Bursar activities, faculty housing finances, and donations to the university. This financial information can be provided by the consumer, initiated by the University, or received from another financial institution. See the University's GLBA-related resources https://it.tulane.edu/guidelines-allcomputer-systems-handling-credit-card-numbers for additional guidance

• The Health Insurance Portability and Accountability Act, complex legislation, and various Rules signed into law in 1996 and updated over the years require safeguarding individually identifiable health information, especially for privacy and security. EPHI is Electronic Protected Health Information that TULANE UNIVERSITY creates, receives, maintains, and/or transmits electronically. It can exist outside a computer, such as on clinical equipment, storage media, tapes, DVDs, and many other peripheral devices. See the University's HIPAA-related resources for additional guidance: https://it.tulane.edu/hipaa-security-policies & https://counsel.tulane.edu/upo/hipaa-privacy-policies-procedures-forms

• The European Union General Data Protection Regulation (GDPR) is a European Union (EU) law that requires organizations that collect data on European citizens to comply with laws regarding protecting that data. In addition, the GDPR gives EU individuals certain rights regarding how their information can be used. See the University's GDPR Privacy Policy for additional guidance: https://tulane.edu/gdpr-privacy-policy

• The Payment Card Industry Data Security Standard (PCI DSS) is a set of requirements issued by the major credit card brands intended to ensure that all entities that process, store, or transmit credit card information maintain a secure environment. Credit/Debit Card numbers and other cardholder information are subject to specific industry standards and additional controls and, thus, must be handled appropriately. See the University's Payment Card Industry Data Security guidelines: https://it.tulane.edu/guidelines-all-computer-systems-handling-credit-card-number