UNIVERSITY OF DENVER	UNIVERSITY OF DENVER POLICY MANUAL DATA CLASSIFICATION	
Responsible Department: Information Technology **Recommended By:** Vice Chancellor of Information Technology, Director of Enterprise Risk Management **Approved By:** Chancellor	**Policy Number** IT 13.10.051	**Effective Date** 12/__/2022

I. INTRODUCTION

The University is committed to safeguarding the information and systems that are critical to the University's mission. In order to establish the foundation for access control policies and procedures, the University has adopted a classification framework for defining the University's data security levels

II. POLICY OVERVIEW

A. University Data shall be classified according to its sensitivity.

B. University Data is classified as Public, Internal, Confidential, and Restricted.

C. The Chief Information Security Officer ("CISO") will establish minimum security requirements proportionate the sensitivity of University Data.

III. PROCESS OVERVIEW

A. Data Classification.

University Data is classified as Public, Internal, Confidential and Restricted.

Public	Internal	Confidential	Restricted
Data is classified as public if the following conditions apply:	Data is classified as internal if the following conditions apply:	Data is classified as confidential if the following conditions apply:	Data is classified as restricted if the following conditions apply:
1. The data is generally available to the public, or The unauthorized use, access, or alteration of the data would not have an adverse impact on the	**1**. The information is proprietary or produced only for use by members of the University community who have a legitimate	**1**. Any information that is contractually protected as confidential by law or by contract and any other information that is considered by the	**1**. Any information protected by federal, state, or local laws and regulations or industry standards, such as CUI, HIPAA, HITECH, the

University or an individual community member.	purpose to access such data **2**. The unauthorized use, access, or alteration of the data could have an adverse impact on the University.	University appropriate for confidential treatment such as FERPA **2.** The data is governed by laws or regulations that require the University to report to the government and/or provide notice to individuals if the data is breached **3.** The unauthorized use, access, or alteration of the data could have a significant adverse impact on the University or an individual community member	Colorado Privacy Act (CPA), similar state laws and PCI-DSS. **2**. The data is governed by laws or regulations that require the University to report to the government and/or provide notice to individuals if the data is breached **3**. The unauthorized use, access, or alteration of the data could have a significant adverse impact on the University or an individual community member

1. Classification of data takes into account the:

a. Inherent attributes of the data;

b. Source of the data;

c. Regulation or policy governing the data; and

d. Relationship of the data to previously disclosed data.

2. The classification of specific data is subject to change as the attributes of that data change (e.g., its elements, content, uses, importance, method of transmission, or regulatory context).

3. The following rules are to be applied when classifying data:

a. When a data element falls into more than one category, it should be classified in the highest applicable category. For example, if a data element meets the definition for both internal and confidential data, it should be classified as confidential.

b. When a data set includes more than one data element, the data set should be classified based on the highest applicable category. For example, if a database contains both public and internal data, the database should be classified as internal.

c. Data may be classified at a higher level than is required by the classifications noted in the chart in subparagraph 4 below; if that is the case, the data element must meet the security measures for the higher classification level.

4. *Data Classification Examples:*

a. The following examples are intended to assist with determining which classification is appropriate for a particular type of data and are not meant to be an exclusive list of data that falls into each classification.

b. Note regarding Research Data: (1) Protected Data Related to Research - Research data which is guided by federal regulation or sponsor requirements: Depending on the subject matter and the data accessed, generated, and/or shared, there may be more stringent requirements from the sponsor, the U.S. federal government, foreign governments, e.g., EU GDPR. Therefore, the data owner is advised to check with Office of Research and Sponsored Programs ("ORSP") or the Institutional Review Board ("IRB") (for human subject research). (2) Except for regulated data such as Protected Health Information (PHI), Social Security Numbers (SSNs), Controlled Unclassified Information (CUI), financial account numbers, and other protected data related to research and systems serving as repositories for these data types, research data predominately falls into the low risk classification. The classification definitions and examples below may be helpful to determine the appropriate risk level to apply.

Public	Internal	Confidential	Restricted
1. Information authorized to be available on or through DU's websites without authentication **2.** Policy and procedure manuals designated by the owner as public **3.** Job postings **4.** University contact information available in the University Directory **5.** Publicly available campus maps **6.** Research data (at data owner's discretion)	**1.** University and employee ID numbers (e.g., University ID) **2.** Personal Data under the GDPR (except for Special Categories of Personal Data) **3.** Unpublished institutional research data, including unpublished research data (at owner's discretion) **4.** University official internal memos and email, non-public reports and policies, budgets, plans	**1.** Human Resources data (e.g., faculty/staff employment applications, personnel files, benefits information, salary, birth date, personal contact information) **2.** Special Categories of Personal Data under the GDPR **3.** Student records (includes FERPA-covered information for educational records) **4.** Non-public contracts **5.** Export controlled information **6.** Donor contact information and non-public gift information **7.** Information received under grants and contracts subject to confidentiality requirements **8.** Law enforcement or court records and confidential investigation records	**1.** Social Security Numbers and national identification numbers **2.** Driver's license numbers **3.** Passport and visa numbers **4.** Operating system passwords, application passwords, and API keys **5.** Central authentication credentials **6.** Personally identifiable health information about patients, including Protected Health Information (PHI) under HIPAA **7.** Unpublished research data that is personally identifiable or identified: Unpublished

		9. Citizen or immigrations status **10.** Unpublished University financial information, strategic plans and real estate or facility development plans **11.** Information on facilities security systems **12.** University intellectual property licensed from a third party or that is contractually restricted	institutional research data, including unpublished research data that is subject to sponsor, federal, or foreign government protected data requirements, including data originating with human subjects or data which are proprietary, confidential, sensitive or designated as controlled unclassified information (CUI). **8.** Credit/Debit card numbers and other cardholder data under the PCI-DSS **9.** Bank/Financial account numbers

IV. DEFINITIONS

A. **“Data”** means information gathered and preserved for reference or analysis. Data includes information used in teaching, research, and administration, and may be preserved in any medium, including, but not limited to, electronic files, paper documents, or film. Data includes originals, as well as all backup and duplicate copies.

B. **“Confidentiality”** requires that data be kept secure and protected from disclosure to and access by unauthorized persons.

C. “**Integrity”** requires keeping data secure, protecting their authenticity, protecting them from improper modification or destruction, and preserving the ability to prove that a given individual created given data.

C. “**Availability”** requires ensuring timely and reliable access to data.

D. **“FERPA”** means the Family Educational Rights and Privacy Act.

E. **“GDPR”** means the General Data Protection Regulation

F. “HIPAA” means the Health Insurance Portability and Accountability Act

V. RESOURCES

A. IT policy - Data Security Standards

B. University Policy IT 13.10.050 – *Institutional Data Management*

C. University Policy IT 2.30.065 – *Data Breach Protocol*

Revision Effective Date	**Purpose**