UTEP Standard 9: Data Classification[1]

This Data Classification Standard shall be used to classify Data. All university data stored, processed, or transmitted on university resources or other resources where university business occurs must be classified into one of the three categories. Based on the data classification you determine for your system, you are required to implement appropriate technical security measures to protect the data consistent with the university Minimum Security Standards. Confidential data has more stringent requirements than Controlled and Published classifications. All systems require some protective measures.

9.1 Definitions and Data Categories.

(a) **CONFIDENTIAL** – Data protected specifically by Federal or State or University of Texas rules and regulations (e.g., HIPAA; FERPA; U.S. Export Controlled information; Sarbanes-Oxley, Gramm-Leach-Bliley; the Texas Identity Theft Enforcement and Protection Act; University of Texas System Policies; specific donor and employee data). University data that are not otherwise protected by a known civil statute or regulation, but which must be protected due to contractual agreements requiring confidentiality, integrity, or availability considerations (e.g., Non-Disclosure Agreements, Memoranda of Understanding, Service Level Agreements, Granting or Funding Agency Agreements, etc.). Previously referred to as Category I.

(b) **CONTROLLED** – Data not otherwise identified as Confidential data, but which are releasable in accordance with the Texas Public Act (e.g., contents of specific e-mail, date of birth, salary, etc.). Such data must be appropriately protected to ensure a controlled and lawful release. Previously referred to as Category II.

(c) **PUBLISHED** – Data not otherwise identified as Confidential or Controlled data (e.g., publically available). Such data have no requirements for confidentiality, integrity, or availability. Previously referred to as Category III.

Note: Any data that is personal to an operator of a system stored on a University Information Resource as a result of incidental personal use is subject to all University policies, standards, procedures, and guidelines. University data stored on non-university information resources must still be verifiably protected according to the respective UTEP Minimum Security Standards for Systems.

[1] Adapted from the "Data Classification Standard" (https://security.utexas.edu/policies/data_classification), with permission from ITS, The University of Texas at Austin, Austin, Texas 78710-1110

9.2 Classification Responsibility. All data owners, data stewards, or designated custodians shall be responsible for classifying Data stored, processed, or transmitted by systems under their purview based on data sensitivity and risk so that the appropriate security controls can be applied and to ensure that the classification is properly maintained in the event the data classification changes. Note that Controlled Unclassified Information (CUI) is a classification designated by the federal government rather than UTEP and must be appropriately protected, marked and labeled in accordance with applicable law, regulations and government-wide policies. The purpose of this standard is to:

(a) educate employees, students, and others who may use Information Resources about their associated responsibilities with such use:

i. by ensuring that the University complies with Federal or State laws, a contract; or

ii. on the demonstrated need to:

- document the integrity of the Data (this, the data has not been altered by either intent or accident);
- restrict and document individuals with access to that Data; and
- ensure appropriate backup and retention of that Data.

(b) Systems storing University Confidential or Data classified by the federal government as CUI will be assessed on an as needed basis in a campus-wide risk assessment where each system is classified based on the Data it is associated with.

9.3 The UTEP Data Classification Standard is to be used to assess Data Confidentiality, Integrity, and Availability (CIA) requirements for Data to be stored or processed within U.T. System Common Use Infrastructure.

9.4 The UTEP Data Classification Standard consists of three mutually exclusive Data classifications based on fit within a spectrum indicating the degree of which access to the Data must be restricted and Data Integrity and Availability must be preserved. The three classifications are as follow:

Data Classification and Description	**Examples**	**Comments**
Confidential Information / Data Information (or Data) is classified as Confidential if it must be protected from unauthorized	Patient billing Information and Protected Health Information subject to HIPAA or applicable state law. Student education records subject to FERPA.	Information (Data) cannot simply be declared to be "Confidential." This classification is reserved for Information that is protected from public release based on State or Federal law, or a legally binding order or

disclosure or public release based on State or Federal law or regulation, and by applicable legal agreement to the extent permitted by law. Previously referred to as Category I Data Please refer to the Extended List of Confidential Data for additional examples. NOTE: This list is not all-inclusive, and does not cover the release of information.	A credit card number associated with an individual's name. A social security number. Medical Research Data that contains protected health information. Certain student loan Information subject to the Gramm Leach Bliley Act. Digital Research (potential human subject data, requirements of granting or funding agency agreements, etc.) Student Information System is considered Confidential because it dictates a high level of uptime. Controlled Unclassified Information (CUI) likely encompasses a moderate to low volume of Data specifically within ORSP and Financial Aid, however other Data may be found in other areas. This Data type involves special handling and compliance requirements, and refers to information that has been classified by the Federal government.	agreement. Likewise, Data cannot be declared to be "Confidential" under all circumstances. Context is an essential element. (In relation to the Federal Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, this category equates to HIGH IMPACT for a Confidentiality, Integrity, and Availability breach.) Data classified as CUI must be protected when CUI is processed, stored, or transmitted by nonfederal organizations using nonfederal systems (i.e. UTEP). UTEP must comply with FIPS 199, FIPS Publication 200, NIST SP 800-53, and NIST SP 800-60. Additionally, please refer to NIST SP 800-171, and the CUI *Registry*. (In terms of FIPS Publication 199, this category equates to MODERATE TO HIGH IMPACT for Confidentiality, Integrity, and Availability breach.)

Controlled Information / Data The Controlled classification applies to Information/Data that is not generally created for or made available for public consumption, but may be subject to release to the public through request via the Texas Public Information Act or similar State or Federal law. Previously referred to as Category II Data	Operational records, operational statistics, employee salaries, budgets, expenditures. Internal communications that do not contain Confidential Information. Research Data that has not yet been published, but which does not contain Confidential Information protected by law.	This classification likely encompasses the greatest volume of Data within the University. (In terms of FIPS 199, this category equates to MODERATE IMPACT for a Confidentiality, Integrity, and Availability breach.)
European Union General Data Protection Regulation (EU GDPR)	GDPR refers to personal data that has been classified by the European Union (EU) as requiring protection. This regulation is designed to enhance data privacy laws to protect and empower all EU citizens' data privacy and reshape the way organizations across the region approach data privacy. Personal data is defined by GDPR as ". . . information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in	This classification likely encompasses a moderate to low volume of Data within the University that expands upon individuals' data rights. This category data equates to MODERATE IMPACT for Confidentiality and Integrity, and LOW for Availability for a breach due to potential, substantial penalties OR for non-compliance.

	technology and the way organisations collect information about people."	
Published Information / Data Published Information/Data includes all Data made available to the public through posting to public websites, distribution through Email, Social Media, print publications, or other Media. Previously referred to as Category III Data	Statistical reports, Fast Facts, Published Research, unrestricted directory information, education content available to the public at no cost.	Information can migrate from one classification to another based on Information life-cycle. Unpublished Research may fit the criteria of "Controlled Information" until published upon which it would become Published Information. (In terms of FIPS 199, this category equates to LOW IMPACT for a Confidentiality, Integrity, and Availability breach.)

9.5 Alternate Method for Classification of Data based on Confidentiality, Integrity and Availability (CIA). If you are evaluating data you are responsible for and it does not clearly fall under the laws and regulations listed in the definition, you can apply the CIA criteria (Most of the legal and regulatory requirements are driven by confidentiality and integrity concerns).

- **CONFIDENTIAL**: The need to strictly limit access to Information / Data to protect the University and individuals from potential loss;
- **CONTROLLED**: Information / Data must be accurate, the users must be able to trust its accuracy.
- **PUBLIC**: Information / Data must be accessible to authorized persons, entities, or devices.

(a) How to Determine Level of Protection. The level of protections applied to a system are determined based on the most confidential data stored in your system. A positive response to the highest category in ANY row is sufficient to place the data into that respective category. Even if the system stores data that could be made available in response to an open records request or information that is public, the entire system must still be protected based on the most confidential data.

Data Classification Weighting

	Confidential	Controlled	Public
Need for **Confidentiality**	Required (High)	Recommended (Medium)	Optional (Low)
	AND/OR	**AND/OR**	**AND/OR**
Need for **Integrity**	Required (High)	Recommended (Medium)	Optional (Low)
	AND/OR	**AND/OR**	**AND/OR**
Need for **Availability**	Required (High)	Recommended (Medium)	Optional (Low)

9.6 UTEP web sites are classified into two distinct groups – **Official** and **Individual** web pages.

(a) **Official** web pages which are permitted are used for:

- official policies and procedures; and
- administrative divisions and offices, academic departments, gran programs, research centers, and other activities or centers authorized by the President or the appropriate Vice President.

(b) **Individual** web pages which are permitted are:

- personal web pages created by faculty, staff and students. Personal web pages must be the responsibility of the page creator, and do not reflect the opinions, positions, policies, or procedures of the University. They must display the name(s) of the creator(s) who assume full legal and ethical responsibility for the content thereof.

NOTE: Anonymous web pages are strictly prohibited.

9.7 Related Policies, Standards, Procedures, Guidelines and Applicable Laws

- UTEP Information Resources Use and Security Policy
- UTEP Information Resources Acceptable Use and Security Policy Agreement
- Extended List of Confidential Data
- Security Exception Reporting Process
- Records and Information Management
- Texas Administrative Code 202
- UT System UTS-165
- European Union General Data Protection Regulation (EU GDPR)
- NIST SP 800-171 Revision 1

9.7 Revision History

First Draft: February 6, 2008
Revised: August 17, 2009
Revised: May 19, 2010
Revised: February 17, 2012
Revised: January 28, 2013
Revised: March 14, 2017
Revised: May 5, 2017
Revised: June 11, 2018 (incorporate information on CUI and GDPR)

Approved: March 16, 2017
Gerard D. Cochrane Jr., Chief Information Security Officer
Approved: May 5, 2017 by CISO
Approved: June 18, 2018 by CISO