

Data Classification Standard

1. Purpose	1
2. Scope.....	1
3. Audience	2
4. Data Classification Standard	2
5. Using C-I-A to Help Classify Data for Which You Are Responsible.....	4
6. Non-Compliance and Exceptions	6
7. Related UT Austin Policies, Procedures, Best Practices and Applicable Laws	6
8. Revision History	6
9. Approvals	9

1. Purpose

This standard serves as a supplement to the [Information Resources Use and Security Policy](#), which was drafted in response to [Texas Administrative Code 202](#) and [UT System UTS-165](#). Adherence to the standard will facilitate applying the appropriate security controls to university data.

The objective of this standard is to assist [data stewards](#), IT [owners](#) and [custodians](#) in the assessment of information systems to determine what level of security is required to protect data on the [systems](#) for which they are responsible. The standard divides data into three categories:

- Category I
- Category II
- Category III

This standard exists in addition to all other university policies and federal and state regulations governing the protection of the university’s data. Compliance with this classification standard will not ensure that data will be properly secured. Instead, this standard should be integrated into a comprehensive information security plan.

2. Scope

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

Data Classification Standard

Document Version: Approved

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. Category-I data has more stringent requirements than Categories II and III. All systems require some protective measures.

Note: Data that is personal to the operator of a system and stored, processed, or transmitted on a university IT resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.

3. Audience

All faculty, staff, student employees, contractors, and vendors working with University of Texas at Austin data.

4. Data Classification Standard

To classify your data, you must start by understanding what the classifications are. There are specific laws and regulations that govern some kinds of data. Additionally, there are situations where you must consider whether the confidentiality, integrity, or availability of the data is a factor. Finally, consider that you may be storing information on more than one system, such as moving data between computers by CD or flash drive, for example. If you rate only your primary computer as Category-I, but not your secondary computer or the transfer media, the secondary computer could put data at risk because it won't be well protected.

4.1. Category-I Data

University data protected specifically by federal or state law 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.) See the [extended list of Category-I data classification examples](#) for specifics."

Examples of How Data Can Be Lost	Impact of Category-I Data Loss
<ul style="list-style-type: none"> Laptop or other data storage system stolen from car. Research Assistant accesses system after leaving research project because passwords aren't changed. Unauthorized visitor walks into unlocked lab and steals equipment or accesses unsecured computer. Unsecured application on a networked computer is hacked and data stolen. 	<ul style="list-style-type: none"> Long-term loss of research funding from granting agencies. Long-term loss of reputation. Published research called into question because data is unreliable. Unauthorized tampering of research data. Increase in regulatory requirements. Long-term loss of critical campus or departmental service. Individuals put at risk for identity theft.

Protect your Category-I data by applying the appropriate Minimum Security Standards.

4.2. Category-II Data

University data not otherwise identified as Category-I data, but which are releasable in accordance with the Texas Public Information 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.

Examples of How Data Can Be Lost	Impact of Category-II Data Loss
<p>In addition to the above scenarios...</p> <ul style="list-style-type: none"> Staff member wanting to be helpful releases information they are not authorized to share. 	<ul style="list-style-type: none"> Short-term loss of reputation. Short-term loss of research funding. Short-term loss of critical departmental service. Unauthorized tampering of research data. Individuals put at risk for identity theft.

Protect your Category-II data by applying the appropriate Minimum Security Standards.

4.3. Category-III Data

University data not otherwise identified as Category-I or Category-II data (e.g., publicly available). Such data have no requirement for confidentiality, integrity, or availability.

Examples of How Data Can Be Lost	Impact of Category-III Data Loss
<p>See the above scenarios.</p>	<p>Loss of use of personal workstation or laptop. Loss of personal data with no impact to the university.</p>

Protect your Category-III data by applying the appropriate Minimum Security Standards.

5. Using C-I-A to Help Classify Data for Which You Are Responsible

If you are evaluating data you are responsible for and it doesn't clearly fall under the laws and regulations listed in the definition, you can apply the Confidentiality, Integrity, and Availability (CIA) criteria. (Most of the legal and regulatory requirements are driven by confidentiality and integrity concerns.)

- **Confidentiality:** The need to strictly limit access to data to protect the university and individuals from loss.
- **Integrity:** Data must be accurate, and users must be able to trust its accuracy.
- **Availability:** Data must be accessible to authorized persons, entities, or devices.

To determine the level of protections applied to a system, base your classification on the most *confidential* data stored, processed, or transmitted by the 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.

	Category I	Category II	Category III
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)

Once you classify data you are responsible for, review the university Minimum Security Standards. These standards describe the appropriate steps for protecting data based on the data classification.

5.1. Data Classification Examples

This section illustrates how the [ISO](#) classifies some familiar data using the CIA (Confidentiality, Integrity, Availability) criteria.

5.1.1. Category-I Data: Web Central

Web Central is considered Category-I data because it is governed by a [service-level agreement](#) that dictates a high level of uptime.

- Need for Confidentiality is optional (low)
- Need for Integrity is recommended (medium)
- **Need for Availability is required (high)**

Since at least one of the CIA conditions is required (high), in this case availability, Web Central is considered Category-I data.

5.1.2. Category-I Data: Digital Research Data with a Funding Agency Agreement

Digital research data is required to be confidential (high) due to various factors, including human subject data, requirements of granting or funding agency agreements, etc. Integrity of the research is required (high) because the data must be accurate and free from errors to be credible. Availability is recommended (medium), because The University of Texas at Austin is not necessarily in any danger or in violation of any law if the data is unavailable for a period of time.

- **Need for Confidentiality is required (high)**
- **Need for Integrity is required (high)**
- Need for Availability is recommended (medium)

5.1.3. Category-II Data: Large Numbers of E-mail Addresses

University e-mail addresses are considered Category-II data. By law they are public information and are published in the university directory (unless restricted by individuals). However, the directory is not intended to be used to harvest e-mail addresses. People must submit open records requests to get e-mail addresses.

- Need for Confidentiality is optional (low)
- Need for Integrity is recommended (medium)
- Need for Availability is recommended (medium)

You may ask yourself why integrity is only recommended and not required. In this case, we are not talking about the source system that stores official e-mail addresses, but the release of that information.

5.1.4. Category-III Data: Professor's Blog

A blog is by its very nature designed to be shared with the world. The confidentiality requirement is therefore optional (low). If the contents of the blog are changed, there would be little to no impact on the ability of the department or the university to carry out their missions. The need for integrity is therefore optional (low). The need for availability is also optional (low) because, should the blog be taken offline for a period of time, the only primary people affected would be the readers of the blog. The department and university should be able to carry on business as usual, while the blog was restored or recreated.

Summary of a professor's blog hosted on a departmental server:

- Need for Confidentiality is optional (low)
- Need for Integrity is optional (low)

Data Classification Standard

Document Version: Approved

- Need for Availability is optional (low)

Since at all of the CIA conditions are optional (low), a professor's blog hosted on a departmental server is considered Category-III data and should be protected using the required and recommended standards for Category-III data.

6. Non-Compliance and Exceptions

Non-compliance with these standards may result in revocation of system or network access, notification of supervisors, and reporting to the Office of Internal Audit.

University of Texas at Austin employees are required to comply with both institutional rules and regulations and applicable UT System rules and regulations. In addition to university and System rules and regulations, University of Texas at Austin employees are required to comply with state laws and regulations.

7. Related UT Austin Policies, Procedures, Best Practices and Applicable Laws

The policies and practices listed here inform the system hardening procedures described in this document; you should be familiar with these documents. (This is not an all-inclusive list of policies and procedures that affect information technology resources.)

[Information Resources Use and Security Policy](#)

[UT Austin Acceptable Use Policy](#)

[UT System \(UTS 165\) Information Resources Use and Security Policy](#)

8. Revision History

Version	Date	New	Original
Data Classification Standard	2/25/2011	Converted web page to PDF	No changes

Version	Date	New	Original
	2/9/2011	<p>Clarified language to bring consistency across policies and standards regarding systems that store, process, or transmit sensitive data, as well as with industry standards and government regulations such as PCI and HIPAA.</p>	<p>II. Scope: All university data stored 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. Category-I data has more stringent requirements than Categories II and III. All systems require some protective measures.</p> <p>Note: Data that is personal to the operator of a system and stored on a university IT resource as a result of incidental personal use is not considered university data. University data stored on non-university IT resources must still be verifiably protected according to the respective university minimum security standards.</p> <p>V. Using C-I-A to Help Classify Data for Which You Are Responsible: To determine the level of protections applied to a system, base your classification on the most <i>confidential</i> data stored in the 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.</p>

Data Classification Standard
Document Version: Approved

Version	Date	New	Original
	11/12/2009	Added UIN to the extended list of Category-I data classification examples. This change was approved by Legal Affairs.	
	10/1/2009	Updated visual appearance to new template. Corrected any out of date links to ensure they are pointing to the most current policy documents.	
	9/14/2007	Changed reference in section I. Purpose to UTS-165. Changed reference in section IV. Data Classification Standard to "University of Texas System Policies" Updated template.	"BMP 53" "University of Texas System Business Procedure Memoranda."
	5/03/2007	Removed the "Funding / sponsorship information" item from the extended list of Category-I data classification examples . This change was approved by Legal Affairs.	
	4/16/2007	Funding / sponsorship information Reorganized content to match other standards documents. Added note in Scope section about personal data stored on a university IT resource.	Same, just organized into appropriate sections. New content.
	11/20/2006	Title changed to "Data Classification Standard" to reflect that this is a requirement. Edited "Guideline" to "Standard" throughout the document and propagated change to all policy documents.	"Data Classification Guidelines"

Version	Date	New	Original
	10/24/2006	New introduction. Revised so definitions are clearly identifiable and tied to what will be in the Handbook of Operating Procedures. Split example from grid for evaluating data.	Entire document has changed. Examples and lists of data that are protected have not changed.

9. Approvals

Name	Role	Members	Date
Chief Information Security Officer	Approval	Cam Beasley	March 3, 2011