



## Data Classification Standards

[Overview](#)

[Category I Data](#)

[Category II Data](#)

[Category III Data](#)

[Classifying Your Data](#)

[Examples](#)

[Conclusion](#)

### Overview

The Data Classification Standards are a tool provided to help information resource owners and custodians assess information systems to determine the sensitivity of the data within the system. The standards divide data into three categories:

- Category I
- Category II
- Category III

All data stored on university resources is to be classified into one of the three categories. Use the following criteria to determine which data category is appropriate for data stored on or manipulated by a particular information or infrastructure system. Owners are responsible for categorizing their data appropriately. Based on the data classification category you determine for your system, you may be required to take additional steps to harden the system in order to protect the data.

The Information Security Office will provide appropriate encryption tools, secure centralized storage, and will consult for other systems and solutions that you may require. You should review the options for protecting the system and choose the appropriate methods.

### Category I Data

Consider the following examples and scenarios when determining the classification level for your data.

**DATA CLASSIFICATION EXAMPLES:** Data protected specifically by federal or state law or University of Texas rules and regulations, for example: HIPAA; FERPA; specific donor, employee, or sensitive research data; *see extended list of Category I data classification examples*; data that is not otherwise protected by a known civil statute or regulation, but which must be protected due to proprietary, ethical, privacy, or criticality considerations.

**LOSS IMPACT SCENARIOS:** Long-term loss of reputation, long-term loss of research funding, increase in regulatory requirements, long-term loss of critical campus or departmental service, unauthorized tampering of research data, loss of any personal or university owned mobile storage device (desktop, laptop, thumb drive, PDA, etc.) containing university data whose release would fall into the loss impact scenarios listed in this section.

**NOTE:** If you are creating a new system that has Category I data, you should inform the Information Security Office. A security review or risk assessment may be required.

## Category II Data

Consider the following examples and scenarios when determining the classification level for your data.

**DATA CLASSIFICATION EXAMPLES:** Data releasable in accordance with the Texas Public Information Act (contents of specific e-mail, date of birth, salary, etc.); data that must be protected due to proprietary, ethical, or privacy considerations. This classification applies even to data that is not otherwise protected by a known civil statute or regulation.

**LOSS IMPACT SCENARIOS:** Short-term loss of reputation, short-term loss of research funding, short-term loss of critical departmental service, unauthorized tampering of research data.

## Category III Data

**DATA CLASSIFICATION EXAMPLES:** Data that might otherwise be considered publicly available, personal Internet browsing data, personal notes, etc.

**LOSS IMPACT SCENARIOS:** Loss of use of personal workstation or laptop, loss of personal data with no impact to the university.

## Classifying Your Data

If you are still uncertain as to how you should classify the data stored on or manipulated by your systems, please refer to the following matrix. The matrix shows the three criteria that are used to define the data category for a given system or set of data. The criteria are Confidentiality, Integrity, and Availability, defined as follows:

- **Confidentiality** refers to the privacy of an asset. Specifically, confidentiality can be defined as which people, under what conditions, are authorized to access an asset.
- **Integrity** can be more difficult to define than confidentiality, as there are two primary properties to consider when evaluating it. First, there is the notion that an asset should be trusted; that is, there is an expectation that authorized users will only modify an asset in appropriate ways. The second part of integrity is that in the event that data is damaged, or incorrectly altered by authorized or unauthorized users, you must consider how important it is that the data be restored to a trustworthy state with minimum loss.
- **Availability** represents the requirement that an asset be accessible to authorized person, entity, service, or device. As a general rule, the more critical data is, the higher its availability ranking will be.

These criteria should be used to determine which data category is appropriate. A positive response to the highest category in ANY row is sufficient to place the data into that respective category.

<b>Data Classification Weighting</b>			
	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)

## Examples

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

**Caveat:** It should be noted that the ratings listed in the examples below are all based on the individual asset. While it is important to identify and rate an asset on an individual basis, it is equally important to look at the other assets that may be affected by a loss in confidentiality, integrity, or availability in the asset being rated.

### Online Library Catalog: Category I Data

The online library catalog has an optional (low) need for confidentiality since the catalog is public and we want students, faculty, staff and visitors to be able to use the library resources. The need for integrity is high because we do not want the catalog to be changed, whether by accident or maliciously. The need for availability is high because there is no paper alternative and the University of Texas at Dallas could experience a long-term loss of reputation and a long-term loss of research funding if the library catalog is unavailable for a period of time.

Summary data classification of online library catalog:

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

Since at least one of the CIA conditions are required (high), in this case both Integrity and Availability, the online library catalog is considered Category I data. Controls to protect the Integrity and Availability of the online library catalog data are required, but controls to protect the Confidentiality of the data are optional.

### Research Data: Category I Data

Sensitive research data is required to be confidential (high) due to various factors, including human subject data, intellectual property rights, large grant funding, etc. Integrity of the research is required (high) because the data must be accurate and free from errors. Availability is recommended (medium), because The University of Texas at Dallas is not necessarily in any danger or in violation of any law if the data is unavailable for a period of time.

Summary of sensitive research data:

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

Since at least one of the CIA conditions is required (high), in this case both Confidentiality and Integrity, research data is considered Category I data and should be protected appropriately.

### Departmental Calendar: Category II Data

A small department's calendaring system that contains faculty and staff member calendars. The need for confidentiality is optional (low) as the calendars are meant to be shared with others. If the calendars no longer accurately reflected meetings and free/busy time, a department would be thrown off. However, the department should be able to recover relatively quickly by finding an alternative method of coordinating with each other, even if the server is unavailable. Again, the department should not grind to a halt because of the failure of the calendaring system. Although there might be a significant short-term impact, the department should be able to recovery relatively quickly.

Summary of a small department's calendaring system:

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

Since at least one of the CIA conditions is recommended (medium), in this case both Integrity and Availability, a small department's calendaring system is considered Category II data and should be protected appropriately.

### **Professor's Blog: Category III Data**

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)
- Need for Availability is optional (low)

Since 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 appropriately.

### **Conclusion**

Your confidentiality, integrity, and availability ratings are most useful in assessing the risk to the assets in your department. It helps create a better understanding of which assets are the most critical, as well as allowing you to prioritize and develop effective actions to protect the assets at risk. Remember, some data, particularly Category I data, must be protected to meet specific criteria.

View the *UTD Minimum Security Standards*. This document describes the minimum requirements for protecting systems based on the type of data they hold.