

VCU - Data Classification Guidelines¹

[Overview](#)

[Category I Data](#)

[Extended List of Category I Data Classification Examples](#)

[Category II Data](#)

[Category III Data](#)

[Classifying Your Data](#)

[Examples](#)

[Conclusion](#)

[Glossary](#)

Overview

The Data Classification Guidelines are a tool provided to help IT [owners](#) and [custodians](#) assess information systems to determine the sensitivity of the data within the system. The guidelines 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 harden the system in order to protect the data. Technology Services provides guidelines for choosing the appropriate encryption tools (forthcoming), secure centralized storage (forthcoming), and other systems and solutions that you may require. You should review the options for protecting the system and choose the appropriate methods.

For each category below, consider the examples and the scenarios when determining the classification level for your data:

Category I Data

DATA CLASSIFICATION EXAMPLES: Data protected specifically by federal or state law or VCU regulations or VCU Health System 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 implementing a new system or application that contains Category I data and it will be stored on a new server, a Security Plan must be prepared for this system. If the data will be stored on an existing server for which a Security Plan already exists, it is not necessary to create a Security Plan for this system. See the VCU Security website for the Security Plan template.

Category II Data

DATA CLASSIFICATION EXAMPLES: Data releasable in accordance with the Commonwealth of Virginia 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.

Data Classification Weighting			
	Category I	Category II	Category III
Need for	Required (High)	Recommended	Optional (Low)

Confidentiality		(Medium)	
	AND/OR	AND/OR	AND/OR
Need for Integrity	Recommended (High)	Recommended (Medium)	Optional (Low)
	AND/OR	AND/OR	AND/OR
Need for Availability	Recommended (High)	Recommended (Medium)	Optional (Low)

Category I Confidential Data at VCU

As indicated in the above matrix, data that is classified as having a high need for confidentiality is Category I data, and the controls to protect this data are required. For other data that is classified as Category I data because there is a high need for integrity and/or a high need for availability, protection is recommended. The Category I confidential data is the same as the data referred to as “sensitive” data in the Virginia Information Technology Agency (VITA) Information Technology Security Policy (SEC 500-02) and Security Standard (SEC501-01) and will be protected in compliance with the requirements of these documents.

Examples of Data Classifications

This section illustrates how some familiar data would be classified 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.

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 recommended (high) because the data must be accurate and free from errors. Availability is recommended (medium),

because the university 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 recommended (high)
- Need for Availability is recommended (medium)

Since the Need for Confidentiality is high, the controls to protect this data are required.

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 the university 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 recommended (high)
- Need for Availability is recommended (high)

Since this data does not have a high need for confidentiality, it is not required to protect the data with the controls required for confidential data. The need for Integrity and Availability are high and therefore the controls to protect the integrity and availability of the online library catalog data are highly recommended and controls to protect the confidentiality of the data are optional.

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 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 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 Minimum Security Standards.

This document describes the minimum requirements for protecting systems based on the type of data they hold.

Definitions of Legally Protected Data (HIPAA, GLBA, and FERPA)

Definition of HIPAA Data

HIPAA (Health Insurance Portability and Accountability Act) places significant privacy and security requirements on health care practitioners and researchers. If HIPAA applies to your department, you will need to take additional steps in your risk analysis and response.

Does your department handle medical information that is combined in any way with one or more of the following personal health identifiers (PHI)? If the answer is “yes,” then HIPAA applies to your department.

1. Names
2. All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census the geographic unit formed by combining all zip codes with the same three initial digits contains less than 20,000 people

3. All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older
4. Telephone numbers
5. Fax numbers
6. Electronic mail addresses
7. Social security numbers
8. Medical record numbers
9. Health plan beneficiary numbers
10. Account numbers
11. Certificate/license numbers
12. Vehicle identifiers and serial numbers, including license plate numbers
13. Device identifiers and serial numbers
14. Web Universal Resource Locators (URLs)
15. Internet Protocol (IP) address numbers
16. Biometric identifiers, including finger and voice prints
17. Full face photographic images and any comparable images; and
18. Any other unique identifying number, characteristic, or code that is derived from or related to information about the individual

Definition of GLBA Data

If your department provides financial services that place you under the security provisions of the federal Financial Services Modernization Act (Gramm-Leach-Bliley Act), which includes regulations to protect consumers' personal financial information, consider the following:

- Do you collect personal financial information pursuant to issuing credit, including credit cards? (Accepting credit does not apply.)
- Do you collect personal financial information pursuant to granting loans?
- Do you collect payments on which interest is paid? (Deferred payment plans that do not charge interest do not apply.)
- Do you broker investments or mortgages?
- Do you provide financial advice for a fee?

- Do you collect personal financial information pursuant to any other “financial product or service”? (Think about the services banks, brokerages and insurance companies provide.)
- Have you negotiated a contract with a financial service provider or do you plan to in the future?

Note: All the practices required by GLBA are also required by HIPAA.

Definition of FERPA Data

FERPA (Family Educational Rights and Privacy Act) restricts access and release of student information. Full information on the University’s FERPA-related policies is at <http://www.students.vcu.edu/rg/policies/privacy.htm>.

Directory information may be released without a student's prior consent; this information is limited to:

- student name
- home and school addresses, telephone numbers, e-mail address
- year of birth
- country of citizenship major(s)
- school of enrollment
- full or part-time status
- year in school
- participation in officially-recognized activities and sports
- dates of attendance
- degrees, honors, scholarships, and awards received
- most recent previous educational institution attended
- names of parents or guardians
- weight and height of members of athletic teams

All other information not specifically listed, including grades, courses, days and times of course meetings, withdrawals, suspension, and month and day of birth, cannot be disclosed without the student’s permission. Such information needs to be protected not only from external release, but also protected from access by

those within the University who do not have an authorized, job-related need to see it.

Glossary

Owners

The authoritative head of the respective college, school, or unit. The owner is responsible for the function that is supported by the resource or for carrying out the program that uses the resources. The owner of a collection of information is the person responsible for the business results of that system or the business use of the information. Where appropriate, ownership may be shared by managers of different departments. The owner or his designated representatives are responsible for and authorized to:

- Approve access and formally assign custody of an information resources asset.
- Determine the asset's value.
- Specify and establish data control requirements that provide security, and convey them to users and custodians.
- Specify appropriate controls, based on risk assessment, to protect the state's information resources from unauthorized modification, deletion, or disclosure. Controls shall extend to information resources outsourced by the university.
- Confirm that controls are in place to ensure the accuracy, authenticity, and integrity of data.
- Confirm compliance with applicable controls.
- Assign custody of information resources assets and provide appropriate authority to implement security controls and procedures.
- Review access lists based on documented security risk management decisions.

Custodian

Guardian or caretaker; the holder of data, the agent charged with implementing the controls specified by the owner. The custodian is responsible for the processing and storage of information. The custodians of information resources,

including entities providing outsourced information resources services to the university, must:

- Implement the controls specified by the owner(s).
- Provide physical and procedural safeguards for the information resources.
- Assist owners in evaluating the cost-effectiveness of controls and monitoring.
- Implement the monitoring techniques and procedures for detecting, reporting, and investigating incident

¹Adapted from “Classification of Data”

(http://www.stanford.edu/group/security/classification/classification_of_data.html),

with permission from Stanford University, Stanford, California 94305-4102.

Last modified January 2008