



UNIVERSITY of  
SAINT FRANCIS™

## **Data Classification Policy**

- I. Policy Statement**
- II. Purpose**
- III. Data Classification Standard**
- IV. Non-Compliance and Exceptions**
- V. Contacts**
- VI. Data Classification Addendum A**

## **I. Policy Statement**

The University of Saint Francis views University data, in all its forms and throughout its life cycle, as an asset of the University, therefore all members of the University community have a responsibility to protect University data from unauthorized access, modification, disclosure, transmission or destruction, and are expected to be familiar with and comply with this policy. Departments should carefully review and assign the appropriate data classification category for their information. Violations of this policy can lead to disciplinary action up to and including dismissal, expulsion and /or legal action. Any known violations of this policy are to be reported to the University's Director or Technology Security and Compliance.

## **II. Purpose**

To educate the University community about the importance of protecting data generated, accessed, transmitted and stored by the University, to identify procedures that should be in place to protect the confidentiality, integrity and availability of University data, and to comply with local, state and federal regulations regarding privacy and confidentiality of information.

## **III. Data Classification Standard**

Data owned, created, used, or maintained by the University will be classified into one of the following categories.

- **Public** – Public data is information that may or must be open to the general public. It is defined as information with no existing local, national or international legal restrictions on access or usage.
- **Internal Use Only** – Internal Use Only data is information that must be guarded due to proprietary, ethical, or privacy consideration, and must be protected from unauthorized access, modification, transmission, storage, or other use. This classification applies even though there may not be a civil statutes requiring this protection. Internal Use Only data is information that is restricted to members of the University community who have a legitimate purpose for accessing such data.
- **Confidential** – Confidential data is information protected by statutes, regulations, University policies or contractual language. Vice Presidents may also designate data as Confidential. Confidential data may be disclosed to individuals on a need-to-know basis only. Disclosure to parties outside of the University should be authorized by executive management such as a Vice President, Provost, University Attorney or University President.

In order to accurately classify University data personnel should use the Confidentiality, Integrity, and Availability (**CIA**) process:

- **Confidentiality:** The need to strictly limit access to data in order 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 classifications on the most confidential 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.

#### Data Classification Weighting

	<b>Confidential</b>	<b>Internal Use Only</b>	<b>Public</b>
<b>Need for Confidentiality</b>	Required (High)	Recommended (Medium)	Optional (Low)
	<b>AND/OR</b>	<b>AND/OR</b>	<b>AND/OR</b>
<b>Need for Integrity</b>	Required (High)	Recommended (Medium)	Optional (Low)
	<b>AND/OR</b>	<b>AND/OR</b>	<b>AND/OR</b>
<b>Need for Availability</b>	Required (High)	Recommended (Medium)	Optional (Low)

Once data has been classified it must be stored in the appropriate manner.

- **Public:** No storage requirements
- **Internal Use Only:** When stored in electronic format, data should be protected with strong passwords to prevent access from persons outside of the University.  
When stored in hard-copy format, data must be stored in a secure area where access by those outside of the University is limited.
- **Confidential:** When stored in electronic format, data must be protected with strong passwords and stored on servers that are physically protected in a UTS accessible space in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.  
When stored in hard-copy format, data must be stored in a locked drawer, room or area where access is controlled by strict physical access control measures to prevent unauthorized access.  
When send via fax, data must be send only to a location that has been verified secure.  
Confidential Data should not be sent via electronic methods unless the electronic method utilizes strong encryption methods.

Each Data Classification Standards require different requirements for disclosure, storage, destruction, and notification requirements if the data is lost or improperly released. Please see the attached addendum (Addendum A) for details. When provided in this policy, examples are illustrative only, and serve as identification implementation practices rather than specific requirements.

Departments should carefully evaluate the appropriate data classification for their information and when in doubt should err on the side of caution.

#### ***IV. Non-Compliance and Exceptions***

Violation of this policy must be reported to the Director of Technology Security and Compliance for the purpose of remediation.

Unauthorized disclosure of Internal Use Only data is a violation of this policy and will result in disciplinary action up to and including dismissal.

Unauthorized disclosure of Confidential data is a violation of this policy and will result in disciplinary action up to and including dismissal, and will be reported to proper legal authorities as required by the situation.

At a minimum, access to network and computer resources will be revoked.

University of Saint Francis employees are required to comply with institutional policies, rules, and regulations. In addition to University of Saint Francis policies, rules, and regulations, University of Saint Francis employees are required to comply with state and federal laws and regulations.

#### ***V. Contacts:***

Security Questions:

Director of Technology, Security and Compliance, 260-399-7700 x 6019

[www.sf.edu/sf/uts/tsc](http://www.sf.edu/sf/uts/tsc)

Reporting an incident:

Director of Technology, Security and Compliance, 260-399-7700 x 6019

[www.sf.edu/sf/uts/tsc](http://www.sf.edu/sf/uts/tsc)

Executive Director of University Technology Services, 260-399-7700 x 6020

[www.sf.edu/sf/uts](http://www.sf.edu/sf/uts)

## Data Classification Addendum A

Data Classification	Public	Internal Use Only	Confidential
<b>Definition</b>	Public data is information that may or must be accessible to the public. Information is not restricted by any existing statute or regulation.	Internal Use Only data is not approved for general circulation outside the organization.	Confidential Data is information protected by statutes, regulations, University policies or contractual language.
<b>Disclosure Guidelines</b>	Public data is subject to University disclosure rules, but is available to all members of the University community and to all individuals and entities external to the University community.	<p>Must not be disclosed to parties outside the organization without explicit management authorization.</p> <p>Must not be posted on a public website.</p>	<p>Must not be disclosed to parties without explicit management authorization.</p> <p>May be disclosed to employees with a direct job function requiring access.</p> <p>Disclosure to parties outside the University should be authorized by executive management such as a Vice President, Provost, University Attorney, or University President.</p> <p>Must not be posted on a public website</p>
<b>Storage Requirements</b>	None	<p>When stored in electronic format, should be protected with strong passwords to prevent access outside the university.</p> <p>When stored in hard-copy format, must be stored in secure area where access by those outside the university is limited.</p>	<p>When stored in electronic format, must be protected with strong passwords and stored on servers that are physically protected in a UTS accessible space in order to protect against loss, theft, unauthorized access, and unauthorized disclosure.</p> <p>When stored in hard-copy format, data must be stored in a locked drawer, room or area where access is controlled by strict physical access control measures to prevent unauthorized access..</p> <p>When sent via fax, data must be sent only to a location that has been verified secure.</p> <p>Confidential Data should not be sent via electronic methods unless the electronic method utilized strong encryption methods.</p>
<b>Destruction Requirements</b>	None	Must be destroyed when no longer needed subject to the <u><i>University's Records Management Policy (In Development)</i></u>	Must be destroyed when no longer needed subject to the <u><i>University's Records Management Policy (In Development)</i></u>

## Data Classification Addendum A

Data Classification	Public	Internal Use Only	Confidential
		<p>Hard Copy materials must be destroyed by shredding or other processes that destroys data beyond either recognition or reconstruction.</p> <p>Electronic storage media shall be sanitized appropriately prior to disposal.</p>	<p>Hard Copy materials must be destroyed by shredding or other process that destroys data beyond either recognition or reconstruction</p> <p>Electronic storage media shall be sanitized appropriately prior to disposal. <u><i>Electronic Equipment Recycling Policy (In Development)</i></u></p>
Notification Requirement	None	The Office of Technology Security and Compliance must be notified in a timely manner if data classified as Internal Use Only has been disclosed outside the university community.	The Office of Technology Security and Compliance must be notified in a timely manner if data classified as Confidential is, or is suspected of being, lost, disclosed to unauthorized parties, or if any unauthorized use of USF information systems has taken place, or is suspected of taking place.
Examples	<ul style="list-style-type: none"> <li>• Publicly posted press releases</li> <li>• Publicly posted schedules of classes or program descriptions</li> </ul>	<ul style="list-style-type: none"> <li>• General Internal memos</li> <li>• General Meeting minutes</li> <li>• Internal surveys and reports</li> </ul>	<ul style="list-style-type: none"> <li>• Social Security Numbers</li> <li>• Protected Health Information</li> <li>• Non-public student data</li> <li>• Personnel records</li> <li>• Any data identified by governmental statute, regulation, or court order to be treated as confidential</li> <li>• FERPA</li> <li>• HIPAA</li> </ul>