University of South Florida

ISSP-001

Data Classification Standard

Code:	ISSP-001
Version:	2.1
Date of current version:	09/16/2018
Last Review:	09/16/2018
Created by:	Alex Campoe - CISO
Approved by:	Sidney Fernandes - CIO
Confidentiality level:	Low

Revision History

Version	Published	Author	Description
1.0	2/7/2018	Alex Campoe	Last update of previous version
2.0	2/27/2018	Alex Campoe	Major reorganization and redefinition of sensitivity classes. Increased number of examples of data, servers, and applications.
2.1	9/16/2018	Campoe	Based on feedback, replaced “sensitivity” with “confidentiality.”

ISSP-001 Data Classification Standard

The University of South Florida is committed to protecting the privacy of its students, alumni, faculty, and staff, as well as protecting the confidentiality, integrity, and availability of information important to the University's mission.

USF has classified its information assets to determine who is allowed to access the information and what security precautions must be taken to protect it from unauthorized access. These measures put in place to adequately ensure the security of electronic data depend on two parameters: the **sensitivity** of the data, and the level of **criticality** of the data. The equipment housing this data inherits the level of criticality and sensitivity of the information it contains. This equipment can be a server, a desktop computer, or a backup tape.

This document offers standards for the classification of electronic resources within the University of South Florida according to their level of criticality and sensitivity.

Confidentiality of the Data

Confidentiality is a measure of how freely the data can be handled and how protected it has to be against unwarranted disclosure or modification.

Low Confidentiality

Controls are not mandated by Federal or State regulations, University policy, or by the data custodian.

The data is intended for public disclosure, or

The loss of confidentiality, integrity, or availability of the data or system would have no adverse impact on our

Medium Confidentiality

If compromised, could have a moderate adverse impact on the University through the mission, financial loss, loss of confidence, or loss of public standing, or

The data is not available to the public.

High Confidentiality

Access and modification of the data are controlled.

Protection of the data is required by law/regulation,

USF is required to self-report to the government and/or provide notice to the individual if the data is inappropriately accessed, or

mission, safety, finances, or reputation.		The loss of confidentiality, integrity, or availability of the data or system could have a significant adverse impact on our mission, safety, finances, or reputation.

Data Confidentiality Classification Examples

Low Confidentiality

NetID

Information authorized to be available on or through USF's websites without authentication

Policy and procedure manuals designated by the owner as public

Job postings

Student Handbook

Class catalog

Directory information, when confidentiality has not been requested

Publicly available campus maps

Medium Confidentiality

Non-public reports, budgets, plans, financial info

Scholarship data

Engineering, design, and operational information regarding Stanford infrastructure

Faculty/staff employment applications, personnel files, benefits, salary, birth date, personal contact information

Non-published research data

High Confidentiality

Health Information, including Protected Health Information (PHI)

Health Insurance policy ID numbers

Social Security Numbers

Credit card numbers

Financial account numbers

Export controlled information under U.S. laws

Driver's license numbers

Passport and visa numbers

Donor contact information and non-public gift information.

Background check information and other FDLE protected data

Server Classification Examples

According to NIST, a server is "a host that provides one or more services for other hosts over a network as a primary function."

Low Confidentiality

Servers that do not access, store, create or transmit any Moderate or High Confidentiality Data

Web servers used to publish public data

Print servers with encrypted cache drives

Web server hosting College class and course information

Research server housing publicly available data.

Medium Confidentiality

Database of non-public University contracts

File server containing non-public documentation

Print servers with non-encrypted drives

High Confidentiality

Servers running the Student Information System (Banner)

Servers running the Human Resources system (GEMS)

Servers housing PHI

Servers housing Social Security Numbers

Servers housing data with FDLE, NIH, or Export Controlled data

Servers controlling access to the USF Network through NetID

Application Classification Examples

Low Confidentiality

+ Application handling Low Confidentiality data

Online Library Catalog

University online catalog displaying academic course descriptions

BullRunner shuttle schedule

Medium Confidentiality

Application handling Medium Confidentiality data

Emergency Notification System

JIRA

Service Desk

High Confidentiality

Application handling High Confidentiality data

Student Information System (Banner)

Human Resources system (GEMS)

Identity and Access Management systems

Alumni Databases

University Policy applications

USF Approved Services

This table indicates which classifications of data are allowed on a selection of commonly used USF IT services.

Service	L	M	H
Audio and Video Conferencing: GoToMeeting, Skype for Business	✓	✓	
Calendar: Office365	✓	✓	✓
Cloud Infrastructure: Microsoft Azure	✓	✓	
Content Management: WordPress	✓	✓	
Database Hosting: MySQL, MSSQL, Oracle	✓	✓	✓
Document Management: AppXtender	✓	✓	✓
Document Management: Box Enterprise	✓	✓	✓
Document Management: Microsoft OneDrive Enterprise, Google Drive Enterprise	✓	✓	
Electronic Signature: Docusign	✓	✓	✓
Email: Google Mail, Outlook 365	✓	✓	
Encryption: Bitlocker, PGP	✓	✓	✓
Instant Messaging: Slack	✓	✓	
Issue Tracking: JIRA Service Desk, ServiceNow	✓	✓	
Survey Tool: Qualtrics	✓	✓	
Voice Messaging: Cisco	✓	✓	
VPN: Juniper Pulse	✓	✓	✓
Wiki: Confluence	✓	✓	

Criticality of the Data

Criticality is a measure of the importance of the data. Criticality deals with the "availability" aspect of the data.

Data considered sensitive may not necessarily be considered critical. Assigning a level of criticality to a data set must take into consideration the answer to a few questions:

1) Will administrators be able to recover the data set in case of disaster?
2) How long will the recovery process take?
3) What is the effect of this downtime, including loss of public standing?

Low Criticality

Data is classified as Low Criticality (LC), also commonly known as "deferrable," if the University can operate without it for extended periods of time.

Medium Criticality

Data is considered Medium Criticality (MC), also known as "required," when it is important to the campus, but University operations would continue for a moderate period even if the data is not available.

High Criticality

Data is considered High Criticality (HC) or "essential" when it is critical to the business of the University. When HC data is not available, even for a brief period of time, or its integrity is questionable, the University will be unable to function. The results could be loss of funds for the University and potential liability.

Data Criticality Examples

Low Criticality

Student Blogs

Email Lists, such as USF-NEWS

Medium Criticality

Student Email

Backend identity data

High Criticality

Authentication data (NetID)

LMS Data

Banner Data

Faculty and Staff Email

Server Criticality Examples

Low Criticality

Departmental web servers

Vulnerability assessment servers

Medium Criticality

Antivirus Management

Log consolidation servers

High Criticality

Domain Controllers

Network Infrastructure

Banner System

Peoplesoft System

File Storage Systems

Application/Service Criticality Examples

Low Criticality

Student Blogs

Email Lists, such as USF-NEWS

Skype for Business

Docusign

Qualtrics

Cisco Voice Mail

Confluence

VZ Orientation – St. Pete

Medium Criticality

Student Email

Backend identity data

AppXtender

Slack

Jira Service Desk

VPN

High Criticality

AD and ADFS

DNS

Canvas

Banner

GEMS and FAST

Box.net

Office365 (Calendar, Email)