USC University of Southern California

Data Classification Standard

Document ID Reference: ST06

Issue Date: 10/30/2020 **Effective Date:** 10/31/2021

DOCUMENT CONTROL

DOCUMENT NAME: Data Classification Standard
DOCUMENT ID REFERENCE: ST06

AUTHORIZATION:

Prepared By	Reviewed By	Approved By
IS GRC Staff	Sandra Taylor	Gus Anagnos
	Director of IS GRC	CISO
Date:	Date: 10/01/2020	Date: 10/30/2020

VERSION HISTORY:

Version	Issue Date	Effective Date	Prepared By	Authorized By	Description
1.1	10/01/2021	10/31/2021	Information Security Governance, Risk & Compliance	Gus Anagnos	Updated definitions Updated formatting
1.0	10/30/2020	10/31/2021	Information Security Governance, Risk & Compliance	Gus Anagnos	Original Version

1.0 Introduction

1.1 Purpose

This document establishes the University of Southern California (USC) approach to effectively identify and classify USC data based on the type of data and the importance the data holds to USC. This standard provides the foundational requirements that the USC schools and units will utilize to effectively classify USC data and the assets that create, use, store, transmit, and archive USC data.

1.2 Scope

This Standard applies to all Covered Individuals listed below:

- University faculty members (including part-time and visiting faculty);
- Staff and other employees, (such as postdoctoral scholars, postdoctoral fellows, and student workers);
- iVIP (guests with electronic access), as well as any other users of the network infrastructure, including independent contractors or others (e.g., temporary agency employees) who may be given access on a temporary basis to university systems; and
- Third parties, including vendors, consultants, and contractors.

This standard applies to all USC data and equipment, including USC student data, whether located at a USC facility or a third-party facility, and whether handled by USC employees, or USC contractors, vendors, third party service providers, or their staff or agents. This standard also applies to all USC schools and units. The guidance in this standard will be considered the minimum acceptable requirements for classifying data within USC. This standard sets forth expectations across the university. Additional guidance and control measures may apply to certain areas of USC. This standard will not be construed to limit application of more stringent requirements where justified by university, school or unit needs or assessed risk.

1.3 Objective

This standard establishes procedures for the management, operation, and security of all data processing facilities and communicate minimum requirements for user behavior in protecting USC information assets.

2.0 Standard Requirements

2.1 USC Data Classification Matrix

The following table outlines the USC classification levels against the types of data that USC creates, uses, stores, transmits, archives, and destroys:

	Confidential	Confidential – Controlled	Internal Use Only	Public
Personal Information	✓			
General Data Protection Regulation (GDPR) information	✓		✓	
Student Information (e.g., FERPA)	✓		✓	
Student Directory Information (as defined by USC Student Records Policy			✓	
Payment Information (e.g., PCI)	✓			
Protected Health Information (e.g., HIPAA)	✓		✓	
Investigations (Judicial)	✓			
Export Controlled Information	✓	✓		
ITAR Information	✓	✓		
Research Information	✓	✓	✓	
Financial Information (e.g., GLBA)	✓		✓	
USC Operating Information	✓		✓	

2.2 Labeling USC Data

In accordance with Section 2.1 of the Data Protection Policy, all forms of data will be classified. This includes, but is not limited to hard copy documents, electronic media, soft copies, assets that contain data, and all storage devices. USC Data will be labeled as one of the following:

- CONFIDENTIAL
    - CONFIDENTIAL – CONTROLLED
- INTERNAL USE ONLY
- PUBLIC

2.3 Personal Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying personal information, which would require special handling based on the requirements set forth under regional and national regulations:

Personal Information	
Definition	Personal information is defined as data that can be used to ascertain the identity of an individual. This data contains details about an individual that defines racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation and is protected under privacy regulations.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the following conditions are met:
	
	• Contains the individual’s name and one of the following attributes:
	  ○ Personal identification number (e.g., Social Security Number, passport number, etc.)
	  ○ Bank account number
	  ○ Biometric data
	  ○ Account and password
	  ○ Driver’s license number
	  ○ Sexual orientation
	  ○ Religious affiliation
	  ○ Ethnicity
	
	INTERNAL USE ONLY
	
	Data and assets will be classified as INTERNAL USE ONLY when the following conditions are met, and the data is not obtainable through public records:
	
	• Contains the individual’s name and one of the following attributes:
	  ○ Contact Information
	  ○ Political affiliation
	  ○ Social organizations
	  ○ USC ID (7 Digit)
	• If there is any combination of one or more attributes from the list above, this may be considered “CONFIDENTIAL”

2.4 Personally Identifiable Information (PII)

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying privacy information, which would require special handling based on requirements set forth under regional and national regulations:

Privacy Information	
Definition	Privacy Information is defined as data that can be used to ascertain the identity of an individual. This data contains details about an individual that defines racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person’s sex life or sexual orientation.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the following conditions are met:
	
	• Contains the individual’s name and any of the following attributes listed:
	  ○ Gender
	  ○ Ethnicity
	  ○ Sexual orientation
	  ○ Healthcare and health insurance information
	  ○ Biometric data
	  ○ DNA
	  ○ Retinal scan
	  ○ Fingerprints
	  ○ Political party
	  ○ Religion
	  ○ Social organizations
	  ○ Trade union membership
	  ○ Philosophical beliefs

Examples of Regulations	• GDPR

2.5 Student Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying student data, which would require special handling based on the requirements set forth under regional and national regulations:

Student Information	
Definition	Student Information is defined as data that is associated with an applicant, admitted candidate or USC student. This data contains details about a student which includes personal, academic and university administrative data.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the following conditions are met:
	
	• Contains the name of the student and any of the following details:
	  ○ Date of birth
	  ○ Gender
	  ○ Sexual orientation
	  ○ Ethnicity
	  ○ Religious affiliation
	  ○ Citizenship
	  ○ Disciplinary status
	  ○ Grade point average (GPA)
	  ○ Marital status
	  ○ Identification Number (e.g., social security number)
	  ○ USC Student ID (10 Digit)
	  ○ Grades and exam scores
	  ○ Test scores (e.g., SAT, GRE, etc.)
	  ○ Progress reports (e.g., STARS)
	
	INTERNAL USE ONLY
	
	Data and assets will be classified as INTERNAL USE ONLY when the following conditions are met:
	
	• Contains the name of the student and any of the following details:
	  ○ Address (local and permanent)
	  ○ Telephone number
	  ○ USC ID (7 Digit)
	  ○ University email address
	  ○ Student photo
	  ○ USC attendance dates
	  ○ USC degrees earned (with dates)
	  ○ Academic honors
	  ○ Major, minor and degree objective
	  ○ Expected date of graduation
	  ○ Previous schools attended
	  ○ Enrollment status (classes the student is enrolled in)
	  ○ Currently enrolled (Yes, No)

Student Information	
	○ Participation in officially recognized activities and sports
Examples of Regulations	• FERPA ○ Both CONFIDENTIAL and INTERNAL USE ONLY FERPA data can be released, in accordance with FERPA, if the student provides their consent. Please consult with your appropriate school/unit privacy leader to understand the data release requirements under FERPA.

2.6 Payment Card Data

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying credit card information, which would require special handling based on the requirements set forth under regional and national regulations:

	Payment Card Data Information
Definition	Payment Card Industry (PCI) information is defined as data that is protected under the PCI regional and national regulations. PCI information contains details about a payment card account that will be protected in accordance with defined requirements.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the following conditions are met:
	
	• Contains the Card Holder Name and any of the following data:
	  ○ Credit Card Account Number
	  ○ Card Verification Value (CVV)
	  ○ PCI Track 1 Data
	  ○ PCI Track 2 Data

Examples of Regulations	• PCI’s Data Security Standard (DSS)

2.7 Protected Health Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying healthcare data, which would require special handling based on the requirements set forth under regional and national regulations:

	Protected Health Information
Definition	Protected health information (PHI) is Information in any format that identifies the individual, including demographic information collected from an individual that can reasonably be used to identify the individual. Additionally, PHI is information created or received by a health care provider, health plan, employer, or health care clearinghouse; and relates to the past, present, or future physical or mental health or condition of an individual.
Identification and Classification Level	**CONFIDENTIAL** Data and assets will be classified as CONFIDENTIAL when any of the following “identifiers” are present and can be used to identify an individual in relation to their health information: Under the HIPAA Privacy Rule “identifiers” include the following: • Names • Geographic subdivisions smaller than a state (except the first three digits of a zip code if the geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people and the initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000) • All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, and 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) • Telephone numbers • Fax numbers • Electronic mail addresses • Social security numbers • Medical record numbers • Health plan beneficiary numbers • Account numbers • Certificate/license numbers • Vehicle identifiers and serial numbers, including license plate numbers

Protected Health Information	
	• Device identifiers and serial numbers • Web Universal Resource Locators (URLs) • Internet Protocol (IP) address numbers • Biometric identifiers, including finger and voice prints • Full face photographic images and any comparable images • Any other unique identifying number, characteristic, or code (excluding a random identifier code for the subject that is not related to or derived from any existing identifier **NOTICE** • Data that has identifiers listed above and is anonymized will no longer be classified as Confidential. • Please note that anonymized PHI may be classified as Research Information. Please consult with the appropriate research leader to determine if anonymized PHI is protected Research Information.
Examples of Regulations	• HIPAA – citation: https://oshpd.ca.gov/wp-content/uploads/2020/10/HIPPA-Identifiers.pdf

2.8 Investigations (Judicial) Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying legal data, which would require special handling based on the requirements set forth by USC OGC:

Judicial Information	
Definition	Judicial information is defined as data that is required as part of criminal court proceedings, civil court proceedings or internal legal investigations. This data will maintain its integrity and authenticity upon receipt of a subpoena or Legal Hold request from USC OGC and the confidentiality, integrity and availability of this data will be maintained until the subpoena or Legal Hold is rescinded.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the data is related to the categories outlined below has not been released to the public by USC, OGC or authorized USC executives.
	
	• Subpoena
	  ○ Federal court issued subpoena
	  ○ State court issued subpoena
	  ○ Provincial court issued subpoena
	  ○ City or county court issued subpoena
	• External investigation
	  ○ Regulatory investigation
	  ○ Criminal investigation
	  ○ Class action lawsuit
	  ○ Civil lawsuit
	• Internal investigation
	  ○ Human resources incident
	  ○ Legal inquiry
	  ○ University disciplinary investigation

2.9 Export Controlled Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying data that is protected from export outside of the U.S., which would require special handling based on the requirements set forth under regional and national regulations:

Export Controlled Information	
Definition	Export controlled information is defined through explicit restrictions on how data can be accessed, transported and shared. This data is restricted under the controls set forth by the Export Control Classification Number (ECCN) that is assigned to USC data and assets by the Department of Commerce and defines the restrictions on who can access the data and where data can be accessed from or transported.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the data is related to the categories outlined and has been deemed to be highly important to USC based on direction from the assigned USC Export Control official.
	
	• ECCNs
	  ○ ECCN LIST
	• EAR99 classification
	• Data types
	  ○ Source code
	  ○ Installer package executable
	  ○ Microsoft Installer (MSI)
	  ○ Applications
	  ○ Dynamic Link Libraries (DLL)
	  ○ Source library files
	  ○ Design drawings
	  ○ Compiled applications
	  ○ Technical documentation
	  ○ Algorithms
	  ○ Models
	  ○ Theorems
	  ○ Methodologies
	  ○ Installer packages
	  ○ Chemical compounds and formulas
	  ○ Metallurgic compounds and alloys
	  ○ Photographs and images
	  ○ Manufacturing instructions
	  ○ Manufacturing processes
	  ○ Laboratory notebooks
	  ○ Research meeting minutes
	• Asset types
	  ○ Physical systems
	  ○ Prototypes
	  ○ Hard copy documentation
	  ○ Loaned equipment

Examples of Regulations	• Export Administration Regulations (EAR)

2.10 Data Transport Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying data that is protected from export outside of the U.S., which would require special handling based on the requirements set forth under regional and national regulations:

Data Transport Information	
Definition	Data Transport information is defined as data that has explicit restrictions on how it can be accessed, transported and shared. This data is restricted under the controls set forth by the U.S. Munitions List (USML) code that is assigned to USC data and assets by the Directorate of Defense Controls (DDTC) and defines the restrictions on who can access the data and where data can be accessed from or transported.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL when the data is related to the categories outlined and has been deemed to be highly important to USC based on direction from the assigned USC Export Control official.
	
	• USML Code
	  ○ USML LIST
	• ITAR USML classification
	• Data types
	  ○ Source code
	  ○ Installer package executable
	  ○ Microsoft Installer (MSI)
	  ○ Applications
	  ○ Dynamic Link Libraries (DLL)
	  ○ Source library files
	  ○ Design drawings
	  ○ Compiled applications
	  ○ Technical documentation
	  ○ Algorithms
	  ○ Models
	  ○ Theorems
	  ○ Methodologies
	  ○ Installer packages
	  ○ Chemical compounds and formulas
	  ○ Metallurgic compounds and alloys
	  ○ Photographs and images
	  ○ Manufacturing instructions
	  ○ Manufacturing processes
	  ○ Laboratory notebooks
	  ○ Research meeting minutes
	• Asset types
	  ○ Physical systems
	  ○ Prototypes
	  ○ Hard copy documentation
	  ○ Loaned equipment

Examples of Regulations	• International Traffic in Arms Regulations (ITAR)

2.11 Research Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying data that is protected under contractual agreements, which would require special handling based on the requirements set forth by USC executives, OOC, OGC and school/unit leadership:

Research Information	
Definition	Research information is defined as data that is developed as part of USC’s research programs and is protected under contractual agreements with public and private entities. Research information may have explicit restrictions on how data can be accessed, transported and shared and this data may be regulated under additional laws. Research information contains intellectual property that developed either solely by USC, in conjunction with other research organizations or subcontracted with public and private entities and the ownership of the intellectual property may be owned by USC, co-licensed with another organization or owned by a third party.
Identification and Classification Level	**CONFIDENTIAL** Data and assets will be classified as CONFIDENTIAL when the data is deemed to be highly important to USC and requires appropriate measures to protect the data based on USC, contractual and/or regulatory requirements. Please consult with the appropriate USC school/unit leadership and stakeholders to determine the appropriate classification to assign to the data and assets. **INTERNAL USE ONLY** Data and assets will be classified as INTERNAL USE ONLY when the data is deemed to be important to USC and requires appropriate measures to protect the data based on USC, contractual and/or regulatory requirements. Please consult with the appropriate USC school/unit leadership and stakeholders to determine the appropriate classification to assign to the data and assets. **NOTICE** • Data, assets and products that are released to a contracted entity who owns the data, assets and products will have the USC classification removed from the data, assets and products prior to delivery. • Data, assets and products that are released to the public will have the USC classification removed from the data, assets and products for public consumption.

2.12 Financial Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying confidential USC financial information, which would require special handling based on the requirements set forth by under regional and national regulations:

Financial Information	
Definition	Financial institutions or companies that offer consumers financial products or services like loans, financial or investment advice, or insurance, are required to explain their data-sharing practices to their customers and to safeguard sensitive data.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL- when the data is related to the categories outlined and has been deemed to be highly important to USC based on direction from OGC, OOC, authorized USC executives or the data owners.
	
	Personal Information Examples
	• Name
	• Date of Birth
	• Address
	• Contact Information
	• Email Address
	• Identification Number
	  ○ U.S. Social Security Number
	  ○ Insurance Number
	  ○ Driver’s license number
	  ○ National Identification Card
	  ○ Passport Number
	
	Financial Information Examples
	• Bank account number
	• ABA numbers
	• Loan information
	• Credit card and debit card information
	• Grant information
	• Non-public Donation amounts combined with identifiable donor information

Examples of Regulations	• Gramm-Leach-Bliley Act (GLBA)

2.13 USC Operating Information

In accordance with Section 2.3 and 2.4 of the Data Protection Policy, “Confidential” information includes regulated data requiring compliance efforts if exposed, while “Internal Use Only” information includes data used to conduct USC business. The following provides the means for identifying internal USC data, which would require special handling based on the requirements set forth by USC leadership:

USC Operating Information	
Definition	USC Operating Information is defined as data that is used by USC to operate, administer, manage and monitor normal university, school and unit functions and activities.

Identification and Classification Level	**CONFIDENTIAL**
	
	Data and assets will be classified as CONFIDENTIAL- when the data is related to the categories outlined above and has been deemed to be highly important to USC based on direction from OGC, OOC, authorized USC executives or the data owners.
	
	Examples are listed below but are not intended to be a comprehensive list:
	• Faculty Evaluations
	• Summer Camp Programming Information
	• Internal business unit documentation
	  ○ Marketing plans
	  ○ Business plans
	  ○ Competitive analysis
	  ○ Audit or assessment findings not requiring disclosure
	  ○ Contracts and contract terms
	  ○ Policies, standards and procedures
	  ○ Routine administrative and office information
	  ○ Intranet content
	• Information Technology
	  ○ IT and Security system designs
	  ○ IT and Security system configurations
	  ○ IT and Security system design requirements
	  ○ Internal IP addresses
	  ○ IT and Security system diagrams and maps
	  ○ Purchased product license keys
	  ○ Internal USC Applications
	• Non-regulated information
	  ○ Telephone directories
	  ○ Organization charts
	  ○ Contact lists
	
	INTERNAL USE ONLY
	
	Data and assets will be classified as INTERNAL USE ONLY when the data is related to the categories outlined above and has been deemed to be of importance to USC based on direction from OGC, OOC, authorized USC executives or the data owners.

	NOTICE Data that is released to the public will have the classification markings removed from the content prior to release of the data.

3.0 Standard Compliance

3.1 Compliance Measurement

The Office of the CISO and the Office of Audit Services will collectively monitor compliance with this standard, USC's information security policies and standards, and applicable federal and state laws and regulations using various methods, including but not limited to periodic policy and standard attestations. Compliance with information security policies and standards will be monitored regularly in conjunction with USC's monitoring of its information security program. Audit Services will conduct periodic internal audits to ensure compliance.

3.2 Exceptions

Any exceptions to the standard will be submitted and approved in accordance with the Information Risk Committee by the OCISO Governance, Risk Management, and Compliance. Exceptions will be requested via Microsoft Forms to the OCISO Governance, Risk Management, and Compliance team.

3.3 Non-Compliance

Violation of this standard may lead to this being classified as a serious misconduct, which is grounds for discipline in accordance with the Faculty Handbook, staff employment policies, and SCampus, as appropriate. Any disciplinary action under this standard will consider the severity of the offense and the individual's intent and could include termination of access to the USC network, USC systems and/or applications, as well as employment actions up to and including termination, and student disciplinary actions up to and including expulsion.

4.0 Related Policies, Standards, and Processes

- Data Protection Policy
- USC Information Security Policies – Terms and Glossary

5.0 Definitions and Terms

- **Confidential**: Data that typically includes regulated data requiring compliance efforts if exposed to unauthorized parties, or would cause legal, financial, reputational, operational harm if disclosed
- **Confidential-Controlled Data**: data is a sub-category of Confidential and is to be used only for Covered Defense Information, which includes Controlled Technical Information (CTI), Controlled Unclassified Information (CUI), or any other data that has military or space application where the data provider (e.g., research sponsor) has imposed safeguarding or dissemination controls for reasons of national security
- **Student Directory Information**: Information contained in the education records of a student that would not generally be considered harmful or an invasion of privacy if disclosed. (e.g., name, address, date and place of birth, dates of attendance, etc.). A school may disclose "directory information" to third parties without consent if it has given public notice of the types of information which it has designated as "directory information," the parent's or eligible student's right to restrict the disclosure of such

information, and the period of time within which a parent or eligible student has to notify the school in writing that he or she does not want any or all of those types of information designated as "directory information."

- **Internal Use Only**: Data that includes all information used to conduct USC business, unless categorized as “Confidential” or “Public”
- **Public**: Data that is not regulated and is generally made available through public interfaces and requires no protection mechanisms
- For more definitions and terms, visit the USC Information Security Policies Terms and Glossary

6.0 Standard Revision

All revisions to this Standard will be made with the approval of the OCISO GRC, Information Risk Committee, and USC General Counsel.

7.0 Standard Acknowledgement

Periodically, all authorized users will be required to read and acknowledge understanding this standard.