SOUTH TEXAS COLLEGE

Information Security Office

P.O. Box 9701• McAllen, TX 78502-9701

Ph. (956) 872-2335 • Fax (956) 872-2344

Data Classification Guidelines

1. PURPOSE

The purpose of these guidelines is to provide additional information to help clarify our data classification standard. We must understand the categories and use the same language across the college. These categories are used to assign risk to an information resource and identify the security measures that will be used to protect it.

2. CLASSIFICATION CATEGORIES AND EXAMPLES

CLASSIFICATION CATEGORY	EXAMPLES
Confidential	• Student academic records (grades, class schedules, and/or GPA) • Personally identifiable information (PII) protected by FERPA or Texas Law (with or without social security numbers) • Federal Tax Information (FTI) • Counseling and health records (HIPAA) • Credit card information (PCI) • Private individual financial information (GLBA) • Aggregate data without disclosure avoidance methods • Departmental data that needs to be kept private • Information that we are bound to protect by a legally binding agreement • Data protected by CJIS (Criminal Justice Information Services) Security Policy • Data classified as Controlled Unclassified Information by the federal government • Information related to security or infrastructure issues for computers, which is confidential through Section 552.139 of the Texas Government Code
Restricted	• Directory data for students that opted out from disclosure • Public information requested outside of the official process
Public	• Course listing information

	• Aggregate data with disclosure avoidance methods • Employee directory • Public information requested through the official process

3. ACCEPTABLE STORAGE METHODS BY CLASSIFICATION CATEGORY

To perform college operations, it may be necessary to share information with other departments or other authorized individuals. It can be difficult to decide whether a method or medium is an acceptable means of sharing the information. Please reference Appendix A for the Acceptable storage reference table, which was created to help you identify the correct place to store data.

4. DEFINITIONS

Personally Identifiable Information (PII)

Personally identifiable information for education records is a FERPA term referring to identifiable information that is maintained in education records and includes direct identifiers, such as a student's name or identification number, indirect identifiers, such as a student's date of birth, or other information which can be used to distinguish or trace an individual's identity either directly or indirectly through linkages with other information.

The term includes, but is not limited to—

(a) The student's name;

(b) The name of the student's parent or other family members;

(c) The address of the student or student's family;

(d) A personal identifier, such as the student's social security number, student number, or biometric record;

(e) Other indirect identifiers, such as the student's date of birth, place of birth, and mother's maiden name;

(f) Other information that alone or in combination, is linked or linkable to a specific student that would allow a reasonable person in the school community, who does not have personal knowledge of the relevant circumstances, to identify the student with reasonable certainty; or

(g) Information requested by a person whom the educational agency or institution reasonably believes knows the identity of the student to whom the education record relates.

Disclosure avoidance

"Disclosure avoidance" refers to the efforts made to reduce the risk of disclosure, such as applying statistical methods to protect PII in aggregate data tables. These safeguards often referred to as disclosure avoidance methods, can take many forms (e.g., data suppression, rounding, recoding, etc.).

5. RELATED GUIDANCE

FERPA – Frequently Asked Questions—Disclosure Avoidance

https://studentprivacy.ed.gov/frequently-asked-questions

U.S. Government Publishing Office – 34 CFR § 99.3
http://www.ecfr.gov/cgi-bin/text-idx?rgn=div5&node=34:1.1.1.1.33

Appendix A – Acceptable storage locations by classification category reference table

STORAGE LOCATION	CONFIDENTIAL	RESTRICTED	PUBLIC
College Computer (Desktop/Laptop)	Only if the disk or the data is encrypted	Only if the disk or the data is encrypted	Yes
College Smartphone/Tablet	Only if compliant with mobile device standard	Only if compliant with mobile device standard	Yes
College Email	No	Yes	Yes
Personal Email	No	No	Yes
Portable Storage (USB/Mobile Device/DVD/CD)	No	No	Yes
IT Network Storage	Yes	Yes	Yes
Secure Share (LiquidFiles)	Yes	Yes	Yes
College Cloud Storage (OneDrive)	Only class-grade books	Yes	Yes
Personal Cloud Storage	No	No	Yes
Personal Computer (Desktop/Laptop)	No	No	Yes
Personal Smartphone/Tablet	Only if compliant with mobile device standards and while employed by STC	Only if compliant with mobile device standards and while employed by STC	Yes
College Website	No	No	Yes
Printed Media/Documents	Only if kept in a secure location	Only if kept in a secure location	Yes