AR 3750.2 Data Classification

Reference(s):

Family Educational Rights and Privacy Act ("FERPA"), 20 U.S.C. §1232g(b), 34 CFR Part 99
National Institute of Standards and Technology (NIST) "Guide to Protecting the Confidentiality of Personally Identifiable Information," Special Publication 800-122
Education Code Section 70902
California Civil Code 1798.29, 1798.82, and 1798.84
Federal Rules of Civil Procedure 16, 26, 33, 34, 37, 45
FTC Regulations 16 CFR 313.3(n), 16 CFR 314.1-5
Gramm-Leach Bliley Act Sections 501, 505(b)(2); U.S. Code 15 USC 6801(b), 6805(b)(2)

Purpose and Scope

The purpose of this Administrative Regulation is to establish requirements for classifying and protecting Rancho Santiago Community College District (RSCCD) data assets.

A data asset is a definable piece of information, regardless of format, that is recognized as valuable to the organization. Classifying information is at the core of an information security program because it specifies how information, based on its sensitivity and value, will be protected from unauthorized disclosure, use, modification, or deletion.

This regulation applies to all RSCCD students, employees and board members and to others granted use of RSCCD's data assets. This regulation refers to all data assets collected, generated, maintained, and entrusted to RSCCD in paper or electronic form, whether individually controlled or shared, whether used for teaching, research, administrative, or other purposes.

Data Classification

Data classification is the process of assigning value to data in order to organize it according to its risk to loss or harm from disclosure. Users of RSCCD systems must understand the importance of securely handling the information that they can access and the standards that have been created to ensure data protection.

Specific protection requirements are mandated for certain types of data, such as credit card information or Payment Card Industry data (PCI), Personally Identifiable Information (PII), Protected Health Information (PHI), and Financial Data. Consistent use of this Data Classification Administrative Regulation will help to ensure RSCCD maintains adequate data protection.

Aggregated and Disaggregated data

Aggregated data is information that combines and summarizes information to provide a high-level overview. Disaggregated data is information that allows for a deeper exploration of specific dimensions within large datasets, helping to understand subsets better.

Responsibilities

RSCCD Designated Data Stewards, as defined in AR 3750.1, have the responsibility to classify the subset of data that they are responsible for. RSCCD Data Trustees have the final authority to classify the data related to the functions managed, administered or run by the units and personnel who report to them or by the Data Stewards designated by them. In the context of data classification, the responsibilities of both Data Stewards and Data Trustees include the following:

- Determining the level of confidentiality that should be assigned to information.
- Working with Information Technology Services (ITS) to select security controls that are appropriate to the level of sensitivity, value or confidentiality of the application or data it processes.
- Ensuring that third parties to whom data has been entrusted meet RSCCD security and data privacy requirements.

Classification of Data Assets

RSCCD classifies information according to its sensitivity and the potential impact of disclosure. In general, information is disclosed when there is a business need-to-know. Information must be consistently handled according to its requirements for confidentiality and disclosure. If the classification level is set too high, the cost of protection will be excessive in relation to the value or sensitivity of the data. If it is set too low, the risk of compromise could be increased. Downgrading to a lower classification at a future date is appropriate should conditions warrant.

Data Classification Categories

Information that is owned, used, created or maintained by RSCCD must be classified into one of three categories:

- Public
- Internal
- Restricted (Confidential)

Public

Public data is information that is suitable for routine public disclosure and use. This type of data is non-sensitive and does not require any special handling, security, or protection measures. The security level for public data is minimal, ensuring its availability to large audiences. Examples of public data may include:

- Publicly accessible web pages
- Academic recruiting materials
- Materials that, by California State law, must be published publicly, including certain academic and grant budgets
- Qualitative data that has been sufficiently anonymized to protect an individual's identity

- Student Educational Records defined as “directory” information on RSCCD’s Board Policy 5040 Student Records, Directory Information and Privacy.
- Disaggregated data that does not contain any Personal Information, as defined within the “Internal” data section in this document
- Aggregated data may include Internal Data as long as aggregation does not allow for identification of individuals. However, in no case shall groups smaller than ten be reported or displayed.

Public data can be freely shared without any restrictions.

Internal

Internal data is information about RSCCD or internal processes that must be guarded due to proprietary or institutional considerations, but which is not classified as sensitive data or otherwise considered confidential. This classification may apply even if there are no regulatory or contractual requirements for its protection.

Data in this category is generally available to employees, contractors, students, or business associates, but is not routinely distributed outside RSCCD. Some Internal data may be limited to individuals who have a legitimate business purpose for accessing the data and not be available to everyone. Examples of Internal data may include:

- Personal Information:
  - Full Names
  - Full Address
  - Telephone Number
  - Email Address
  - Signature
  - Religious or Philosophic beliefs
- Demographics:
  - Race
  - Ethnicity
  - Date of Birth (excluding students who are a member of an athletic team)
  - Place of Birth
  - Gender
  - Sexual Orientation
  - Residency and Citizenship data
- Student Educational Records not defined as “directory” information on RSCCD’s Board Policy 5040 Student Records, Directory Information and Privacy, such as
  - Grades
  - Courses taken
  - Schedule
  - Test Scores
  - Counseling records
- RSCCD internal procedures, forms, and manuals
- Data which is on the internal Intranet, but has not been approved for external communication
- Internal presentation materials

Restricted (also called Confidential)

Restricted data is information that is sensitive in nature, and may be proprietary, personally identifiable, or otherwise be sensitive. Unauthorized compromise or disclosure of the information would be likely to cause serious financial, legal, or reputation damage to RSCCD, or result in embarrassment or difficulty for RSCCD, its trustees, employees, or students.

Restricted data may be protected by statutes, regulations, or contractual requirements. Disclosure is limited to those within RSCCD on a "need-to-know" basis only. Disclosure to parties outside of RSCCD must be authorized by appropriate Data Trustees and may need to be covered by a data protection or data sharing binding agreement. Examples may include:

- Government-issued Identification number:
    - Social Security Number
    - Taxpayer Identification Number
    - Passport Number
    - Driver's License or other federal/state issued identification number
- Financial Data:
    - Account Number
    - Credit or Debit Card Number
    - Credit Report Information
    - Personal Identification, Password or password that would permit access to an individual's financial account
    - Check if access, transmitted or stored by Supplier to deliver the Goods and/or Services Personally identifiable (as defined below) information of our employees, contractors, or students
    - ISIR FTI Data
    - Data that requires Payment Card Industry data (PCI)protection requirements
- Precise Geolocation Data:
    - Precise personal location data obtained from cell tower or Wi-Fi triangulation techniques or latitude, longitude coordinates obtained through GPS technology if such data is sufficiently precise to locate an individual or device.
- Personal Characteristics:
    - Photographic images (particularly of face or other identifying characteristics)
- Biometric data:
    - Retina scans, voice signatures or facial geometry
    - Fingerprints
    - Genetic data
- Medical information:
    - Individual's medical history, mental or physical condition, medical treatment, or diagnosis by a healthcare professional
    - Data qualified as Protected Health Information (PHI)
- Health Insurance data:
    - Individual's health insurance policy number or subscriber identification number
    - Any unique identifier used by a health insurer to identify an individual
    - Any information in an individual's application and claims history, including any appeals records
- Audit reports or results that expose information security configurations or controls
- System and network configuration details, including diagrams, passwords, programs or

other IT-specific documentation

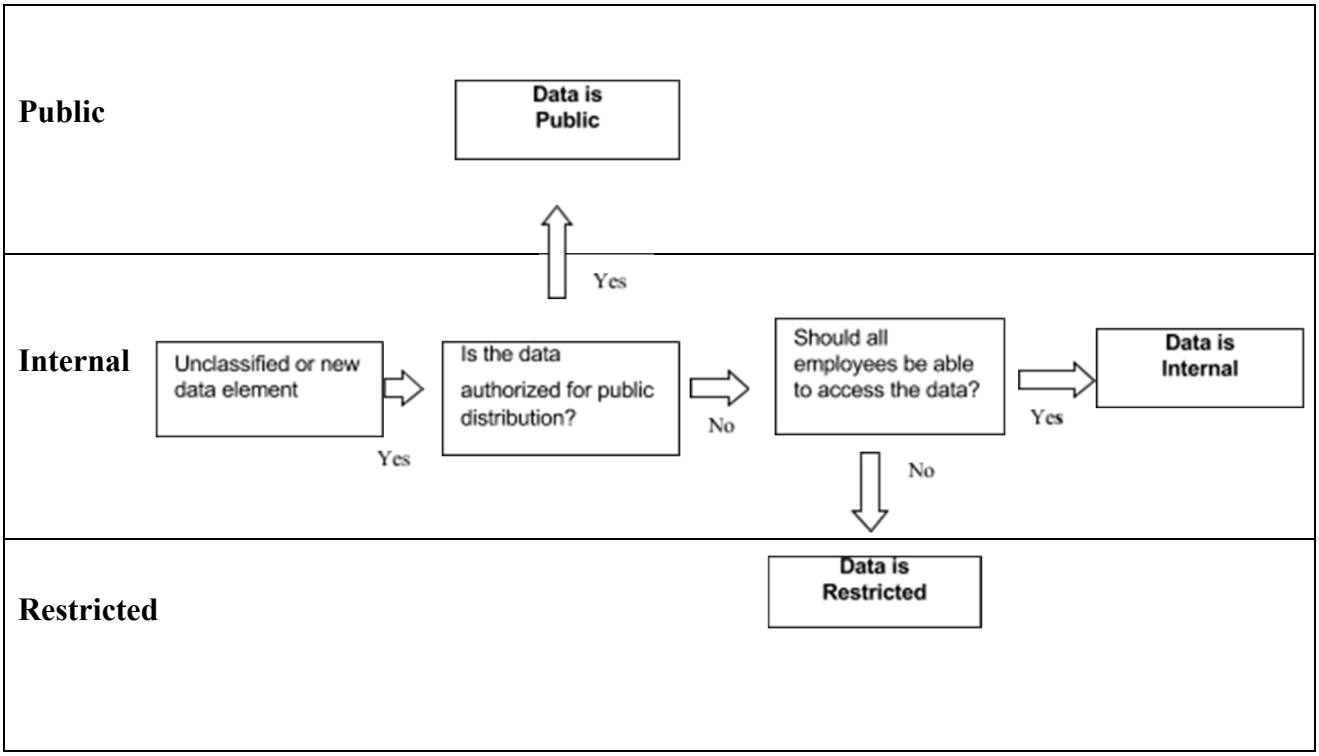
- Personally Identifiable Information (PII): Defined as an individual's first name and last name or first initial and last name in combination with any one or more items classified as Restricted data. However, Personally Identifiable Information shall not include information that is lawfully obtained from publicly available information, or from federal, state, or local government records lawfully made available to the general public.

Minimum Classification

All information should be assumed *Internal* unless classified otherwise.

Classification Flow Chart

The Classification Flow Chart below is intended to assist a Data Trustee, Data Steward, document creator or user to assist in quickly determining the classification of a data element or document.



Adopted: **November 2, 2026**