DATA CLASSIFICATION STANDARD

Purpose and Background:

The Contra Costa Community College District collects, stores, and utilizes data from various sources. To apply the appropriate security protocols for safeguarding the data, this standard establishes a framework for classifying the District's institutional data assets into one of three levels: (1) confidential, (2) sensitive/internal use, and (3) public. It includes protocols for handling data based on its classification to ensure appropriate security measures are applied. The goal is to maximize the use of District data to support academic and administrative objectives while providing a consistent approach to data protection and compliance with applicable laws and regulations.

This classification standard does not alter public information access requirements. California Public Records Act or Federal Freedom of Information Act requests and other legal obligations may require the disclosure or release of information from any category.

Scope:

This standard applies to all institutional data, electronic or non-electronic, which is processed, created, collected, stored, or archived by the District. Any individual or affiliate organization that uses, stores, or transmits District Data shares the responsibility to safeguard such data appropriately.

Classification Criteria and Levels:

This standard categorizes data based on its sensitivity and the potential risks associated with unauthorized exposure, alteration, deletion, or unavailability. The classification guides the implementation of appropriate security measures to protect the data.

Data must be classified based on the highest sensitivity level of any element within it. For example, if a dataset includes a student's name and an optional Social Security number, it should be classified as Confidential Data, even if the name alone has a lower classification. At the same time, data should not be classified more restrictively than necessary for its context.

Classification Description: Level 1 – Confidential

Protected Data

Access, storage, and transmission of confidential information are subject to restrictions as described in the Data Protection Protocol. Information will be classified as confidential if it meets at least one of the criteria below:

a. **Exposure Poses a Severe Risk**
   Confidential data includes information whose unauthorized access, use, disclosure, modification, loss, or deletion could pose a significant risk to the District, its students, employees, or partners. Failure to protect this data may lead to financial loss, reputational damage, or legal consequences for the District.

b. **Legal Obligation**

Information for which disclosure to persons outside of the institution is strictly governed by State or Federal statutes to protect the privacy of an individual's information. California civil codes **1798.29, 1798.82, and 1798.84** require the District to notify affected parties in the event of a data breach of certain private information.

c. **Other Confidential Information**
Information deemed highly sensitive by the District is typically reserved solely for use within a specific department or limited to employees with a specific need to know.

Examples of Confidential information include but are not limited to:

- Passwords or credentials that grant access to Confidential and Internal Use data
- Social Security Numbers (SSN) and name
- Birth date combined with SSN and name
- Citizenship information and name or SSN
- Credit card numbers with cardholder name
- Tax ID with name
- Driver's license number, state identification card, or other forms of national or international identification (such as passports, visas, etc.) in combination with name
- Private key (digital certificate)
- Personnel records
- Criminal background check results

Classification Description: Level 2 – Sensitive/Internal Use

Protected Data

Access, storage, and transmissions of sensitive/internal use information is subject to restrictions as described in the Data Protection Protocols. Information may be classified as sensitive/internal use if it meets at least one of the criteria below:

a. **Sensitive Nature of Data**
Information that must be protected due to proprietary, ethical, contractual, or privacy considerations.
b. **Exposure Poses a Moderate Risk**
Information that may not be specifically protected by statute, regulations, or other legal obligations or mandates but for which unauthorized use, access, disclosure, acquisition, modification, loss, or deletion of could cause financial loss, damage to the college's reputation, violate an individual's privacy rights, or subject the institution to legal action.

Examples of Sensitive/Internal Use information include, but are not limited to:

Identity Validation Keys (when combined with a person's name)
- Birth date (full: mm-dd-yy)
- Birth date (partial: mm-dd only)

Personal Information
- Home address

- Personal telephone numbers
- Personal email address
- Employee evaluations
- Race and ethnicity
- Sexual orientation
- Parents' and other family members' names
- Birthplace (City, State, Country)
- Gender
- Marital status
- Images of individuals shared without their consent

Student Information — Educational Records not defined as "directory" information as defined in FERPA and Board Policy 3013, typically:

- Grades
- Courses taken
- Schedule
- Test scores
- Advising records
- Educational and student services received
- Disciplinary actions

Various Identifiers — Educational Records not defined as "directory" information as defined in FERPA and Board Policy 3013, typically:

- Location of critical or protected assets
- Licensed software
- Vulnerability/security information related to the District
- District or college attorney-client communications

Classification Description: Level 3 – Public

Information at this level requires no specific protective measures. Information that may be designated by the District or by State or Federal statute as generally available and/or intended to be provided to the general public.

Disclosure of this information does not expose the District to financial loss or jeopardize the security of the District's information assets. The unauthorized disclosure, alteration, or destruction of public data should result in little or no risk to the District.

Examples of Public information include, but are not limited to:

- Information on public websites
- Course schedule and catalog
- Job postings
- Salary schedule
- Consumer information

Data Protection Protocols – Confidential and Sensitive Data

- **Data Storage** - Confidential and Internal Use data must be stored exclusively on District-managed IT systems and devices. Storing or archiving confidential or internal use data on personal devices, external cloud storage, flash drives, or third-party platforms is strictly prohibited.
- **Sharing Data/Files with Authorized Individuals**
  - If confidential or sensitive information must be shared, use only approved collaboration tools such as Microsoft Teams, OneDrive, and SharePoint. Configure the shared document so that it is shared with specific individuals rather than anyone who accesses the link.
  - Do not send sensitive or confidential data via email unless you encrypt the email message.
- **Downloading Documents –** Download documents containing confidential and sensitive/internal data only when needed. Do not save them on a laptop for longer than necessary. When possible, leave the data in a centralized, managed system (e.g., Colleague, SQL Reporting Services, SharePoint) rather than downloading data.
- **Use of Generative Artificial Intelligence (AI)** – Do not enter confidential or sensitive data into tools that use generative AI. These tools may process and store input data in ways that are not fully transparent or controlled, increasing the risk of unintended data exposure or breaches. Many AI tools retain user inputs to improve their models, potentially exposing sensitive information to unauthorized parties.
- **Printing –** Print only when absolutely necessary. Do not leave material unattended on printers/copiers and shred documents prior to disposal.

Responsibilities

Everyone who interacts with institutional data is responsible for safeguarding such data appropriately and understanding the data classification categories. District Data Owners are responsible for formally classifying data in their functional areas so that appropriate safeguards are applied. It is appropriate for the Data Owner to be informed of applicable regulations and or confer with subject matter experts who possess in-depth knowledge regarding specific information assets.

Common examples of Data Owners are included below.

Description	Common Data Owner(s)
Student Records	Admissions and Records Directors
Financial Aid Data	Financial Aid Directors
Employee Records	Human Resources
Research Data	Dean of Research and Planning
Financial Data	Chief Financial Officer and College Business Officers

Data Owners should regularly review the classification of their District Data to ensure it remains appropriate based on changes in legal or contractual obligations, as well as shifts in the dataset's use and value to the District.

If a classification change is identified, a security assessment must be conducted to determine whether adjustments to existing protections are needed. Any necessary security updates should be implemented promptly to align with the new classification.

Historical Annotation:
Adopted: 04/15/2025

Related Board Policy:
Board Policy 3013

Related Procedures:
Administrative Procedure 1900.01
Business Procedure 10.06
Student Services Procedure 3026