

RANCHO SANTIAGO COMMUNITY COLLEGE DISTRICT

[Website: Technology Advisory Group](#)

Agenda for December 4, 2025

2:30 p.m. - 4:00 p.m.

<https://rsccd-edu.zoom.us/j/84722067242>

1. Proposal to rename Course Catalog in Self Service (10 minutes) – Howard
2. Agentic AI browser automation and academic dishonesty (10 minutes) – James
3. First reading – AR 3750.X Data Classification (15 minutes) – Gonzalez
4. Technology Update – Colleges
 - SACTAC – Steffens (10 minutes)
 - SCCTEC – Rodriguez (10 minutes)
5. Student experience with technology:
 - SAC – Oberschlake (10 minutes)
 - SCC – Hughes (10 minutes)
6. Approval of TAG Minutes – November 6, 2025 (5 minutes) – **ACTION** – Gonzalez
7. Technology Project listing, November 2025 (5 minutes) – Howard

Next TAG Committee Meeting: February 12, 2025

The Rancho Santiago Community College District aspires to provide equitable, exemplary educational programs and services in safe, inclusive, and supportive learning environments that empower our diverse students and communities to achieve their personal, professional, and academic goals.

Rancho Santiago Community College District
ADMINISTRATIVE REGULATION
Chapter 3
General Institution

AR 3750.X 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 procedure applies to all RSCCD students, faculty, and staff and to others granted use of RSCCD's data assets. This procedure 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.

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

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
- Student Educational Records not defined as “directory” information, 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

Access controls for Internal data should be reviewed at least every two years, and business and data access justification may be required.

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
- Intellectual property
- 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.

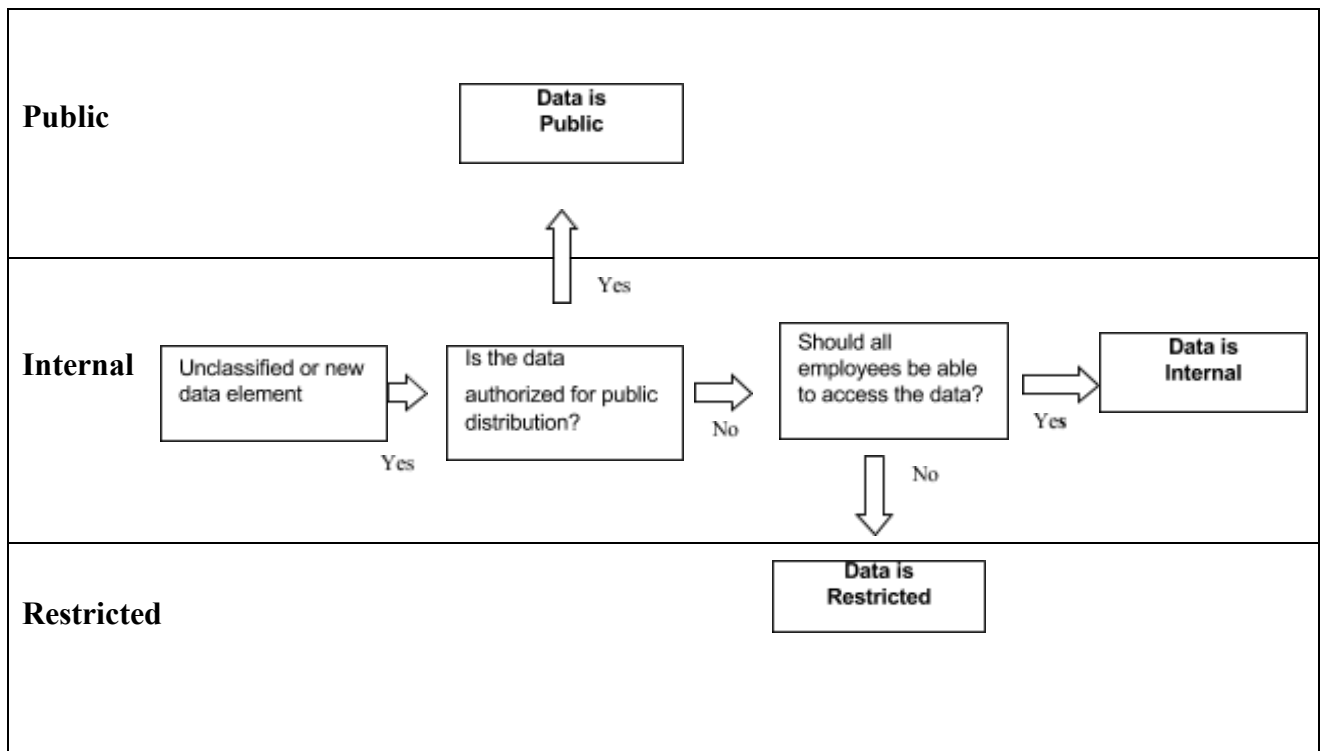
Access controls for Restricted data should be reviewed annually, and business and data access justification are required. All Restricted data must be protected with encryption.

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: (date)

Technology Advisory Group
Zoom Meeting (Invitation shared via Outlook)
2:30 p.m. – 4:00 p.m.

Meeting Minutes for November 6, 2025

Voting Members Present: Song Graham, Jesse Gonzalez, Jennifer McAdam, Alex Natale, Raelyssa Sanchez – SAC Student, Phillip Hughes – SCC Student

Voting Members Absent: Robert Bustamante, Scotty James, Jimmy Nguyen, Sergio Rodriguez, John Steffens, Vangee Oberschlake – SAC Student

Supporting Members: Dane Clacken, Marvin Gabut, Ron Gonzalves, Adam Howard, Kimberly Perna

Discussion

Call to Order

- The meeting was called to order by Mr. Gonzalez at 2:31 PM.
1. Proposal to rename Catalog in Self Service:
 - Mr. Howard provided a brief overview. Shared screen and linked to Self Service, Course Catalog navigation process. Implementation plans after registration, and an actual date will be announced. TAG members provided positive feedback on this update. Request to convey to respective constituents.
 2. Districtwide Accessibility Workgroup update: Mr. Gonzalez provided an overview and update. The ACMM assessment was conducted through the State Chancellor's Office to evaluate how we produce and support accessible digital content. The resulting reports for the district and the colleges will be shared with college councils and the district council. With new federal accessibility requirements taking effect in April 2026, the work group plans to resume efforts to address the findings and plan next steps.
 3. Technology Update – Colleges:
 - SACTAC: Mr. Natale provided an update.
 - Faculty DE Coordinator announcement: SAC Academic Senate DE Coordinators will request disabling AI-generated rubrics and AI grading tools in Canvas until they are fully vetted.
 - Committee goals for the year were reviewed and approved. Review of 2026-2030 strategic plan is ongoing, and the working documents are available on the SACTAC Teams site.
 - Digital Dons hotspots checkouts for students currently have no backlog. 400 computers were purchased through the Digital Divide grant.
 - Library lockers are now available and in use on SAC campus. Previous EBSCO access issue has been resolved.
 - On going discussions on campus alerts to students for (ICE) presence on campus.
 - Ongoing Professional Learning Committee sessions on AI. Next session, Nov. 14th and Nectar AI workshop scheduled the week of convocation. Districtwide AI PD group led by Mr. Natale and Ms. Ponzello; next session Nov. 21st.
 - DE office is working on a retention dashboard tool for faculty chairs of online degree pathways. Transition from PlayPosit to WeVideo is underway. Khanmigo AI tutoring integration in Canvas is in progress.

- ITS updates: Windows 11 updates nearly complete (20–30 devices remaining). Pay-to-Print system will be integrated across campus centers by June 2026 and major AV upgrades planned for 36 classrooms at CEC and I building projected April 2026. Tech replacement plan continues to move forward.
 - Evaluation is ongoing regarding extending Starfish usage. Nuventive and Nectar AI are being used to support program review.
 - Mr. Gonzalez shared additional updates related to Windows 10 devices and recent districtwide email: Remaining Windows 10 devices may be blocked for security; users should contact the Help Desk if they can't connect. Older devices will be covered through replacement.
- SCCTEC:
 - New website updates: Ms. Perna reported that the new website is planned to launch on December 15. The testing and feedback phase is beginning, with the preview link expected to be shared with the campus community shortly.
4. Student experience with technology:
- SAC: Ms. Sanchez reported on the Wi-Fi being experienced inside the gymnasium and Building D. Mr. Gonzalez provided an insight. If students are using the guest network instead of the student Wi-Fi, it can cause dropped connections and slower speeds. Using the student network provides more stable and faster access, so students are encouraged to use that option. Will also have the Infrastructure team to follow up with this issue at SAC.
 - SCC: Mr. Hughes presented results from a Wi-Fi survey conducted at SCC on October 21–22, with 64 student responses.
 - Over half of students rated the Wi-Fi as poor or somewhat poor, mainly affecting mobile devices, laptops, and tablets. Problem areas included the first floors of A and E buildings, D building, H building, the gym, courtyards, and the perch area. Wi-Fi issues were reported to disrupt classes, assignments, online research, emails, and streaming. Nearly 80% used student Wi-Fi, with many, noting problems when texting or calling.
 - Mr. Hughes and Senator Connor Tsai plan to present these findings to the ASG Senate for further discussion.
 - Additional feedback: Students requested better, more stable, and secure Wi-Fi.
 - Mr. Hughes also noted adding survey questions about mobile providers, construction, past Wi-Fi experiences, and gathering more responses, especially from long-term faculty for better insight. Mr. Hughes plans to expand the Wi-Fi survey with his senator and Rob Gustamante.
 - Mr. Gonzalez asked to receive the results and provided positive feedback and offered support, while Kimberly Perna commended the survey's usefulness for troubleshooting.
5. Approval of TAG Minutes – October 2, 2025.
- Mr. Gonzalez made a motion, moved by Ms. Graham and seconded Mr. Natale. Motion passed.
6. Technology Project listing, October 2025: Mr. Gonzalez provided updates on behalf of Mr. Howard. Project trends show 50% completion vs. new project received monthly.
- RG542 Visualization for Chancellor: In coordination with district Research, logic is being reviewed. Determining implementation cycle to go-live.
 - Series 25 Scheduling/Calendaring platform implementation: Project team of 15 participants has been formed, and scheduling for the project kickoff.
 - Colleague 320 implementation: Draft comparisons with current and standardized methods and collaboration with Fiscal. Findings to be presented to the colleges once available.

- XGENED Data Copy: Currently reviewing process to ensure they align with Cal-GETC and preparing to decustomize as they transition to a SaaS model for the Colleague student information system.
- Catalog Hours Cap on WebAtt Batch Uploads: New project aims to ensure accurate unit and grade calculations during batch uploads and web attendance. Development is complete; the team is ready for testing and feedback.
- Add Gen Ed Area filters to Course Search in Self Service: Coordinating testing with Self Service implementation team.
- Inactivate dormant student accounts: IT security related. A process is being developed with Admissions; next step: implement and automate inactivation based on program status.
- VPAT Repository: Near completion. Finalizing additional updates.
- Budgeting tools/Position Control Pilot: Kickoff meeting held. Workgroup within Fiscal and H/R with assessment of criteria next.
- Colleague Self Hosting in AWS private cloud: Proof of concept for Colleague self-hosting is in motion with successful initial testing. We were able to negotiate a 2-year contract extension with Ellucian and ITS aims to maintain the Self Hosting environment as a fallback option if needed.

Informational Handouts

1. Technology Project listing for October 2025

Next Meeting Reminder: December 4, 2025, via Zoom

Adjournment: The meeting was adjourned at 3:32p.m.