Rancho Santiago Community College District
KEY AND ELECTRONIC ACCESS CONTROL PROCEDURE

I. Purpose: To ensure the safety, security, and accessibility for students, employees, and visitors of Rancho Santiago Community College District ("RSCCD" or "District") by implementing key and electronic access control practices in accordance with Board Policy and Administrative Regulation 3501. Safety shall supersede convenience.

II. Definitions: Refer to *Appendix A*.

III. Applicability: This procedure is applicable to all RSCCD properties and employees.

IV. Procedures:

A. Maintaining Security:

1. RSCCD mechanical keys, electronic access control cards and/or electronic fobs ("access credential") are property of the District and shall be surrendered in accordance with Section F below.
2. The District generally maintains a locked door policy to enhance personal safety for all members of the RSCCD community and secure the moveable physical assets of the District. The locked door policy will ensure spaces are able to achieve lock down in an expedient fashion to safeguard the occupants against any unwelcome intruders. Locked door policy is further defined as follows:
   a. All perimeter building entry doors and restrooms shall be unlocked by Maintenance & Operations and remain unlocked during business hours.
   b. Where emergency lockdown devices are present, doors shall remain locked at all times and emergency lockdown device shall be engaged to ensure an expedient lock-down can be achieved.
   c. Where access control and emergency buttons are present, doors may remain unlocked while in use and relocked upon completion of use. If desired, doors may be set to an automatic schedule tied to course scheduling and/or hours of operation.
3. Employees are expected to obtain authorization for assignment of their own access credential(s) to maintain proper access to required buildings. Employees shall ensure any keyed entry into a space opened by said employee is secured after entering or exiting to prevent unauthorized entry.
4. RSCCD personnel who have been granted access credentials shall keep them in a safe and secure place before, during, and after work. Storing access credentials in an unsecured work area (desk, cabinet, closet, etc.), in other unsecured areas, or in personal or District assigned vehicles is unacceptable due to high risk of theft.
5. Access credentials shall not be duplicated or modified by anyone other than

authorized personnel. California Penal Code Section 469 states,

> *"Any person who knowingly makes, duplicates, causes to be duplicated, or uses, or attempts to make, duplicate, cause to be duplicated, or use, or has in his possession any key to a building or other area owned, operated, or controlled by the State of California, any state agency, board, or commission, a county, city, or any public school or community college district without authorization from the person in charge of such building or area or his designated representative and with knowledge of the lack of such authorization is guilty of a misdemeanor."*

6. To protect the integrity of District sites, access credentials assigned to employees or contracted personnel shall not be loaned, signed-out, or transferred to anyone including other employees, students, volunteers, contractors, or vendors.

7. Managers shall ensure that any personnel on an extended absence from work (20 working days or more) such as sick leave, leave of absence, military leave, industrial accident, or any other approved leave of absence, return their mechanical key(s) into the site's associated District Safety and Security Office for safe storage until the employee returns to work.

B. Responsibilities: Refer to *Appendix B*.

C. Mechanical Keys:

1. Maintenance and Operations, Information Technology Services, Facilities Planning, Construction and District Support Services, and District Safety and Security personnel may check out mechanical keys on a daily basis, as needed. Keys shall be returned to a secured District approved drop box within each department upon completion of the employee's shift. Each of the above supervisors within each department are responsible to inventory daily and ensure proper return of mechanical keys at their associated site(s).

2. All master mechanical keys, (AL-1 through AL-5), must be accounted for and inventoried annually by the site's associated District Safety and Security Office and reported to the Chief of Safety and Security (or designee).

3. Any personnel that are assigned an AL-2 (G-GM) mechanical key shall keep the key(s) tethered to them on a lanyard or a clip and chain.

4. Mechanical key cutting requirements:

   a. All blank, uncut keys, and key machine vise jaw, shall be stored in a secured area within the associated site's District Safety and Security Office or Locksmith room. Access to the secured area shall be limited to the Chief of Safety and Security (or designee) and the Locksmith.

   b. District Safety and Security Office shall maintain records of each key cut with the following information 1) date, 2) requester's name, 3) quantity, 4) key stamp, and 5) key code. These records shall be maintained in addition to keeping an inventory of keys within the Key

Management Software.

D. Eligibility:

1. Eligibility for access credentials is determined by business necessity. Access permissions shall be in accordance with *Appendix C*.
2. The Chief of Safety and Security (or designee) shall have control to distribute keys as necessary during emergency situations.

E. Process for Issuance of an Access Credential:

1. Receiving any access credential will require a valid form of identification shown to District Safety and Security Office prior to issuance. Employees shall refer to *Appendix D* for additional procedures on the issuance of access credential(s) for the legacy Sargent Keyso key system, Medeco key system, and electronic access control cards.
   a. All adjunct faculty will be required to return their mechanical keys at the end of their assignment.
2. Contractors and vendors with a verified work contract with RSCCD shall have a District employee submit a request for access credentials. Refer to *Appendix D*. Refer to *Appendix E* for a copy of the forms for the legacy Sargent Keyso system.
   a. All access devices checked out daily from a key box shall be returned daily to the assigned key box upon completion of the work shift.
3. New Medeco Key System and Electronic Access Cards – District Safety and Security is responsible for the implementation and management of the Medeco key system and electronic access cards. All requests for access control credentials must be submitted through the District's Key Management Software. This platform is accessible via the Employee Intranet under the District Safety & Security section. For detailed procedures on submitting a request, refer to *Appendix D*.
4. Legacy Sargent Keyso System – The College Maintenance & Operations department is responsible for the management of legacy Sargent Keyso keys, furniture, and equipment keys, used throughout the District. For detailed procedures on submitting a request, refer to *Appendix D*.
5. If a request for access credential issuance is approved, all employees shall be subject to section G below.

F. Returning and Collecting Keys:

1. When personnel depart employment, their access credentials are to be returned to the site's corresponding District Safety and Security Office prior to departure. A receipt will be provided to employee upon return of keys. Human Resources will require receipt for proof of return as a condition of final exit interview and completion of returning District property.
2. When an employee changes positions, relocates to a new office, or undergoes any similar transition, a new access credential request must be submitted in accordance with Section E above. New access credentials

will only be issued after the originally issued access credential(s) is returned to the District Safety and Security Office.

G. Key Loss or Failure to Return:

1. District Safety and Security Office shall be notified if a key is reported lost, stolen, or not returned by an employee utilizing the *Lost, Stolen, or Unreturned Access Credential Report Form 3*. Refer to *Appendix E* for a copy of the form.

2. District Safety and Security Office will make a determination if an area needs to be rekeyed due to a missing or lost key. Employees who lose a key may be assessed a lost key penalty fee and/or may be subject to disciplinary action. Refer to *Lost, Stolen, or Unreturned Access Credential Report Form* 3 for applicable fee schedule. New keys will not be issued until assessed fees are paid.

3. Contractors/Vendors: In the event keys are not returned, the contractor/vendor acknowledges and assumes the responsibility of the costs to re-key associated RSCCD property due to key loss. A minimum penalty fee of $10,000 shall be assessed for any missing or lost master key.

H. Physical Access Control Cards:

1. Access control cards shall be retained through the District Safety and Security Office.

2. Access control cards shall always be used (where access control exists) in lieu of a mechanical key, unless there is a failure of the access control system.

3. Although not displayed on the access control card, the access control card has expiration dates registered in the access control system. Scheduling predetermined access control card expiration dates serves as a precautionary security measure that encourages regular evaluation of active/inactive cards. Expiration dates are established as follows:

   a. Requests for expiration date extension shall be issued to the associated site's District Safety and Security Office utilizing the *Access Credential Authorization Form*.

I. Form Updates:

1. District Safety and Security Office has authorization to update forms as needed.

2. Employees shall download the most current version of the forms on the Employee Intranet under District Safety and Security.

J. Future Administrative Regulation Updates:

1. This Administrative Regulation is subject to a future revision after all legacy keys are replaced with the Medeco key system.

APPENDIX A – DEFINITIONS

Access Control – Control of entry to an area by any means (generally mechanical or electronic).

Access Credential – A mechanical or electronic device, including but not limited to a key, an access ID card or electronic disk (fob), or combination lock that is used to control access to RSCCD facilities or property.

Requestor – Appointed position that is authorized in the key management system to request keys for their department or area.

Supervisor – Administrator, dean, or manager that the individual requiring access reports to.

Key Records – includes any key codes and/or pinning records.

Mechanical Key (or Key) – Any mechanical device used to operate a mechanically controlled mechanism for entry to a controlled area. These locks may be individually keyed or operate with a building master key.

Physical Access Control Card – An electronic device (also a District issued ID Badge) used to open/close doors.

Site Administrator – This individual shall review and approve all access control credential requests for their assigned department or site. The titles responsible at each corresponding site are Vice President of Administrative Services (main campus and associated satellite site(s)); Vice President of Continuing Education (for adult education centers); and Assistant Vice Chancellor of Facility Planning, Construction and District Support Services (District Office and associated satellite site(s)). Refer to Appendix B, Responsibilities.

Medeco Key System – This is the District's new key system, designed to meet higher security standards and a new master key system. The District Safety & Security department is responsible for the implementation and management of the Medeco key system.

Legacy Sargent Keyso System – This is the District's original key system, currently being phased out and replaced by the new Medeco Key System. The Maintenance and Operations Department oversees its management during the transition.

Key Management Software – This is the District's new key management software used to manage its entire inventory of Medeco keys in accordance with this policy.

APPENDIX B – RESPONSIBILITIES

Employee	**Supervisor**	**District Safety and Security**	**Maintenance and Operations**	**Information Technology Services**
• It shall be the responsibility of all employees to adhere to these procedures • Initiate and secure *Access Credential Authorization Form 1* approvals • Maintain and secure access credentials • Report stolen, lost, or unreturned access credentials	• Shall open the building areas of responsibility for employees who do not have keyed access. District Safety and Security will back up the manager in cases where the manager is unavailable. • Shall ensure employees are requesting appropriate access levels in accordance with this procedure • Maintain current list of department employees who have active access credential authority for issuance to District Safety and Security upon request	• Administer AR3501 • Monitor and manage functionality of access control system • Access controlled buildings: program and update, as required, automatic lock/unlock schedule for access controlled doors • Provide final approval of all *Access Credential Authorization Form 1* requests • Input authorized access credentials into access control software • Provide ongoing maintenance and any required repair of key core for both legacy Sargent Keyso system and the Medeco key system • Mechanical Keys – purchase, store, cut, and issue all keys for the Medeco key system • Oversee Locksmith and Access Technician(s)	• Unlock and relock all perimeter doors, gates, and restrooms in accordance with site's hours of operations • Provide ongoing maintenance and any required repair of doors • Provide ongoing maintenance and any required repair of access control devices • Provide ongoing maintenance and any required repair of door hardware (excluding key core) • Manage and issue furniture and equipment keys • Mechanical Keys – purchase, store, cut, and issue all keys for the legacy Sargent Keyso system	• Manage virtual server(s) • Assist in providing third party vendors access, when required, to server/software • Create and maintain link between Active Directory and other third party integrations • Provide access control software updates

APPENDIX C – ELIGIBILITY

Type	Access Level	Eligibility to Carry / Use	Approval(s) Required
District Master Great-Great Grand Master (GG-GM)	**AL-1** Opens all locks **district-wide**	**Not to be issued or distributed**	**Not to be issued or distributed**
Site Master Great Grand Master (G-GM)	**AL-2** Opens all locks within **one site**	Chancellor; Vice Chancellors; Presidents; Vice Presidents; Assistant Vice Chancellors; Chief of Safety; Lieutenants; Directors of Physical Plant & Facilities; Maintenance Supervisors, Facilities Planning Directors and Managers; ITS Directors	Supervisor; Division VP or Assistant VC; Site Administrator; and Chief of Safety and Security (or designee)
Building Master Grand Master (GM)	**AL-3** Opens all locks within **one building**	Deans; Associate Deans; Directors; Managers; designated M&O, ITS, Facilities, and Safety and Security employees (on a shift basis only)	Supervisor; Division VP or Assistant VC; Site Administrator; and Chief of Safety and Security (or designee)
Room Type Master (MK)	**AL-4** Opens a given group of locks within a building	Employee requiring access to these areas	Supervisor; Division VP or Assistant VC; Site Administrator; and Chief of Safety and Security (or designee)
Unique Room	**AL-5** Opens one lock or two or more locks keyed alike (generally within one building)	Employee requiring access to these areas	Supervisor; Division VP or Assistant VC; Site Administrator; and Chief of Safety and Security (or designee)

APPENDIX C – ELIGIBILITY *(CONTINUED)*

EXAMPLES OF PROPER ACCESS CREDENTIAL DISTRIBUTION:

<u>Non-Access Controlled Buildings</u>:

Scenario A – Faculty member teaching lecture & lab in same building:

1. **Common Area Key** (AL-4)
2. **Lab/Prep Room Key** (AL-4 or AL-5)
3. **Storage Key** (if applicable) (AL-4 or AL-5)
4. **Office Key** (AL-5)

Scenario B – Faculty member teaching lecture in one building and lab in another:

1. **Common Area Key** for BUILDING 1 (AL-4)
2. **Common Area Key** for BUILDING 2 (AL-4)
3. **Lab/Prep Room Key** for BUILDING 2 (AL-4 or AL-5)
4. **Storage Key** (if applicable) (AL-4 or AL-5)
5. **Office Key** (AL-5)

Scenario C – Dean key(s) for each building included in area of responsibility:

1. **Building Master Key** (AL-3)

Scenario D – Administrative Secretary keys:

1. **Common Area Key** (AL-4) for each building included within Division's area of responsibility
2. **Lab/Prep Room Key(s)** (AL-4 or AL-5), as required
3. **Office Key** (AL-4)
4. **Storage Key** (AL-4)

<u>Access Controlled Buildings:</u>

Scenario AA – Faculty member teaching lecture & lab in same building:

1. **Access Control Card** with access credentials to assigned locations in BUILDING 1 including, but not limited to: classrooms, associated lab(s), associated storage/prep, faculty suites, learning centers, conference rooms, etc.
2. **Office Key** (AL-5)

Scenario BB – Faculty member teaching lecture in one building and lab in another:

1. **Access Control Card** with access credentials to assigned locations in BUILDING 1 and BUILDING 2 including, but not limited to: classrooms, associated lab(s), associated storage/prep, faculty suites, learning centers, conference rooms, etc.
2. **Office Key** (AL-5)

Scenario CC – Dean:

1. **Access Control Card** with access credentials to each building included in area of responsibility
2. **Building Master Key** (AL-3) for each building included in area of responsibility

APPENDIX C – ELIGIBILITY *(CONTINUED)*

EXAMPLES OF PROPER ACCESS CREDENTIAL DISTRIBUTION:

Scenario DD – Administrative Secretary:

1. **Access Control Card** with access credentials to each area required within division's n area of responsibility
2. **Office Key(s)** (AL-4)

The following room types shall maintain limited access credential distribution:

- Utility rooms (electrical, mechanical, machine room, etc.)
- Custodial rooms
- MDF / BDF / IDF rooms (ITS network rooms)
- Restrooms
- Building perimeters (unless building is using an access control system)
- Chemical storage rooms
- Cadaver rooms

APPENDIX D – STEPS FOR ISSUANCE OF ACCESS CREDENTIALS

MANAGED BY DISTRICT SAFETY & SECURITY– MEDECO KEY SYSTEM AND ACCESS CONTROL CARDS

Step	Employee	Requester	Supervisor	Site Administrator	District Safety and Security
1.	Request access credential authorization from department key/card requester				
2.		Authorized department requester fills out online request			
3.		Key Management System sends an e-mail to employee's direct supervisor for approval	Supervisor receives email from RSCCD Keys@rsccd.edu notifying them to log into the Key Management System and approve/deny key/card request.		
4.				Site Administrator receives email from RSCCD Keys@rsccd.edu notifying them to log into Key Management System to approve/deny key/card request.	
5.					Approved key/card request will be in Key Management System queue for Safety & Security to process and issue key/card to employee.
6.	Employee receives e-mail from RSCCD Keys@rsccd.edu that the key/card is ready for pick-up.				

7.	Employee signs for and picks up mechanical key(s) and/or cards at corresponding site's Safety and Security office.				Safety and Security issues key/card through Key Management System to employee.

APPENDIX D – STEPS FOR ISSUANCE OF ACCESS CREDENTIALS

MANAGED BY MAINTENANCE AND OPERATIONS – SARGENT KEYSO KEY SYSTEM (LEGACY KEYS)

Step	Employee	Supervisor	Division VP / Assistant VC	Site Administrator (see definitions)	District Safety and Security
1.	Fill out *Access Credential Authorization Form 1* (refer to *Appendix E* for a copy of the form)				
2.	Email form to Supervisor for signature/approval				
3.		Review employee's *Access Credential Authorization Form 1* and confirm conformance with AR 3501			
4.		Approve or deny request and email to next required reviewer: **AL-2 through AL-5** = VP/Assistant VC **AL-1 =** Chief of Safety and Security	**AL-2 through AL-5**: Review employee's *Access Credential Authorization Form 1* and confirm conformance with AR 3501		
5.			Issue approved form to Site Administrator or denied form to Supervisor	**AL-2 through AL-5**: Review employee's *Access Credential Authorization Form 1* and confirm conformance with AR 3501	
6.				Issue approved form to Maintenance & Operations office or denied form to Supervisor	**AL-2 through AL-5**: Review employee's *Access Credential Authorization Form 1* and confirm conformance with AR 3501
7.					**Mechanical Key:** Prepare key within 72 hours and notify employee when available to pick-up at corresponding site's Maintenance & Operations office
8.	Pickup mechanical key(s) corresponding site's Maintenance & Operations office				

APPENDIX E – FORMS

Refer to the subsequent pages for samples of the following forms:

1. *Legacy Sargent Keyso System - Access Credential Authorization Form 1 (Employees Only)*
2. *Legacy Sargent Keyso System - Vendor Access Credential Authorization Form 2*
3. *Legacy Sargent Keyso System and Medeco - Lost, Stolen, or Unreturned Access Credential Report Form 3*

The latest versions of the required forms are available on the Employee Intranet under District Safety and Security.