# AP 3508 Building Access Control

**References: None**

This procedure supports the college's mission while maintaining personal safety and building security and provides for a safe and secure learning and working environment for students, employees, and visitors. This procedure applies to all facilities owned and or operated by Rogue Community College (RCC). Building access control is accomplished by combining opening and closing building times and using keys and electronic access devices.

RCC will issue keys and/or electronic access credentials to employees and persons or organizations with contractual agreements with the college. Keys will not be issued to students in any capacity. Electronic access credentials may be issued to student employees on a case-by-case basis where a specific need exists.

Risk Management is responsible for selecting an electronic access control system in coordination with the Information Technology Services (IT) and Facilities Management, Planning, and Construction (FMPC) Departments that provides for the long-range sustainability of the college.

Keys and/or electronic access credentials should only be issued to individuals with legitimate and official access needs and who have acquired the appropriate approvals. Key access approval rests with the Director of FMPC in consultation with the requestor's supervisor. Approval for electronic access credentials rests with the Director of Risk Management in consultation with the requestor's supervisor.

All keys and electronic access credentials issued shall remain the property of RCC not the individual. They must be returned to the Risk Management Department (electronic access credentials) or FMPC (keys) upon the separation of employment or change of employment, office move, etc., by the employee's direct supervisor or HR.

The Risk Management, IT, and FMPC Departments will review all plans and requests for installing and expanding electronic access control.

RCC buildings are assigned one of the following levels of access control:

- Level A – Doors are automatically unlocked and locked electronically during business hours, which vary, or class schedules, as shown in the college scheduling software by Risk Management. . Individual departments must notify Risk Management if changes are needed so that unlock, and lock schedules can be adjusted.

- Level B – Doors are not equipped with electronic access control. They are unlocked and locked by Campus Security based on class schedules and events shown in the college scheduling software or on a predetermined schedule. This would include certain classrooms, exterior building doors, doors leading into common areas, etc.

- Level C – Doors are on access control and always locked.

- Level D – Doors remain on a key and are not equipped with electronic device access. The individual assigned to the space is responsible for unlocking and locking the space.

- Level E – Doors remain locked and require electronic device credentials and PIN access.

- Level F – Certain exterior doors remain locked and require a perimeter key not in circulation and must be checked out from FMPC.

General-purpose classrooms that only contain tables and chairs and are accessed using a key will be unlocked by Campus Security 30 minutes before a class starts and locked 10 minutes after the class ends unless another class or event is scheduled in the space within the next hour. This is based on the information in the college scheduling software. If Campus Security receives a phone call from an RCC employee asking them to unlock a classroom earlier, they will respond and open the door as soon as possible.

Classrooms that contain any other items such as computers, lab equipment, chemicals, electronics – not including media stations at the podium, specialty equipment, etc. and are accessed using a key or electronic access credentials will be unlocked 10 minutes before class starts and locked 10 minutes after class ends. This is also based on the information in the college scheduling software. If Campus Security receives a phone call from an RCC employee asking them to unlock a classroom earlier, they will respond and open the door as soon as possible.

Any general-purpose classroom accessed using electronic access credentials will be unlocked 30 minutes before the class begins . The doors will automatically lock electronically 10 minutes after the last class ends.

Departmental requests for unlocking a building for a special event must be submitted via the room reservation process, with a follow-up email to Risk Management. Operating hours will be adjusted as necessary for these approved college events.

Scheduled Holidays or Closure Days – All RCC buildings will be locked on days the college is officially closed for Scheduled Holidays, Closure Days, and weather-related or

emergency reasons. Pre-authorized electronic device access for employees will remain unchanged on these days.
Departmental Responsibilities:

Risk Management

- The Director of Risk Management and the Assistant Director of Risk Management are the Electronic Access Control Application Administrator's responsible for managing and coordinating the college's electronic access control system for all existing buildings and for all new buildings that may be constructed in the future, for designing the room access groups to ensure the accountability of electronic access credentials that are issued and removed to maintain an accurate and complete database and to collaborate with other stakeholders, including Southern Oregon University, that require electronic access credentials to perform their duties. The Director of Risk Management shall collaborate with the Chief Information Officer (CIO) and the Chief Facilities Management Officer (CFMO) to align electronic access credentials and key control procedures and practices.

Human Resources

- The Human Resources Department is responsible for issuing all new employee electronic access credentials, including taking the employee's picture and issuing the electronic access credential to the employee. The Human Resources Department will email the Director of Risk Management, the Assistant Director of Risk Management and the employee's supervisor each time an employee electronic access credential is issued so that Risk Management can activate and program the electronic access credential. Human Resources will also notify Risk Management when an employee separates from employment.

Facilities Management, Planning, and Construction

- The Director of FMPC is responsible for managing and coordinating the college's key control program.

- The FMPC Department is responsible for installing, maintaining, and repairing the electronic access control infrastructure and hardware in coordination with Risk Management and IT.

IT

- The installation, maintenance, repair, and upgrade of the server(s) and application software will reside with the IT Department, which will work directly with Risk Management, FMPC, and vendors when necessary.

Supervisors

- Supervisors are responsible for identifying the key and electronic access credential level their employees are authorized to possess, consistent with this Administrative Procedure. Supervisors are responsible for requesting keys through the FMPC Department. Supervisors are responsible for requesting electronic access credential privileges or changes through the Director of Risk Management and Assistant Director of Risk Management.

Keyholder Responsibilities (Key and/or Electronic Access Device)

- Take appropriate measures to safeguard any college keys or electronic access credentials issued to you.
- Never loan anyone your key(s) or electronic access credentials.
- Never use your key(s) or electronic access credentials to grant access to secured areas to non-authorized individuals.
- Never prop open or otherwise disable any normally secured doors.
- Never store key(s) or electronic access credentials in an unsecured fashion.
- Immediately report any lost or missing electronic access credentials to the Director of Risk Management and the Assistant Director of Risk Management.
- Immediately report any lost or missing keys to FMPC.

**Guidelines for Requesting Access**

Electronic access credentials

Requests for electronic access credentials will be made by the employee to the employee's supervisor.

Key Access

The Access Requestor must submit a key request to FMPC for processing.

Contractor keys or electronic access credentials may be issued to the FMPC Department and/or the IT Department annually to facilitate daily contractor work. Keys must be requested from the FMPC Department via the key request process with

appropriate approvals. Requests for electronic access credentials for contractors working for the FMPC Department or IT Department must be submitted to the Risk Management Department via email. The department administrator must facilitate control of the keys and electronic access credentials issued to contractors. Contractors may be responsible for the cost of re-keying locks that may have been compromised due to the non-return of keys issued to the contractors.

Lost or Stolen Keys/ Electronic access credentials

The Keyholder must immediately report stolen, lost, or misplaced key(s) to FMPC and electronic access credentials to the Risk Management Department via email.

FMPC may issue replacement key(s), and Risk Management may issue replacement electronic access credentials upon appropriate approval.

Return of keys or electronic access credentials

For current employees, obsolete, outdated, or unneeded keys must be returned to FMPC.
When no longer employed by the college or holding the role, responsibilities, and/or position for which the key/ electronic access credentials were granted, all associated keys must be returned to HR or the employee's supervisor, who will then turn keys into FMPC and electronic access credentials to Risk Management. Risk Management will cancel electronic access credentials..

Employees should **never** turn over their keys to their coworkers or employees taking their place.

Document Retention

All documentation will be maintained in accordance with Oregon Revised Statutes, as applicable.

**Rescinds Policy Number: None.**

**Approved: April 2, 2024**

**Revised: February 10, 2024**