Clackamas Community College

Responsible Officer:
Responsible Office: College Safety
DRAFT VERSION **1** – 11/01/2019

ELECTRONIC ACCESS CONTROL POLICY

I. Policy Statement

Clackamas Community College (CCC) is committed to the safety and security of all members of the campus community. The college demonstrates this commitment by securing its facilities and physical spaces while striving to maintain a welcoming and hospitable campus environment and allowing as much freedom of access as possible to the general public.

II. Reason for Policy/Purpose

This policy accomplishes the following college objectives, it:

- Establishes access hours and security procedures for campus buildings;
- Helps ensure the safety of CCC faculty, staff, students and visitors;
- Helps prevent crime;
- Helps protect CCC infrastructure, property and other assets; and,
- Establishes authorities and procedures for access control during normal day-to-day campus operations, after-hour access and special events.

III. Applicability

This policy applies to all CCC locations, organizations, and departments as well as all users of CCC facilities and those working on behalf, or at the behest of CCC. It is applicable to all CCC used, owned or controlled facilities, rooms, and enclosures.

IV. Definitions

Access Control: The ability to regulate or restrict building access via a centralized electronic control system.

Electronic Access Control System: All electronic systems used by the College to control, manage and administer access to CCC facilities, rooms and enclosures. Systems include all hardware, firmware, software and campus infrastructure used for electronic access control purposes.

Electronic Access Devices: Access cards and other electronic access devices that allow or control entry into CCC facilities, rooms and enclosures, etc.

Authorized Approver: The Dean of each department, the Vice President of Instruction and Student Services or Vice-President of College Services will coordinate with College Safety to manage Access Control issues. Authorized Approvers have the authority to allow special electronic access requests when they are made by faculty or staff.

Information Technology Services (ITS): All ITS hardware, firmware, software and network infrastructure required to operate campus access control system.

Master Access: This level enables access to every building and specific high security areas.

College Identification Card: The authorized college identification (ID) card used to electronically access campus facilities.

V. Policy

1. Authority

1.1 **Ownership of Access Devices and Codes:** All access control devices issued under this policy are the property of CCC.

1.2 **Administration of Electronic Access Control Systems:** College Safety is responsible for administration and oversight of card access and security for all CCC facilities. Campus Services is responsible for issuing and managing keys used to access CCC facilities. College Safety may delegate some or all of their responsibility to other campus departments to accommodate specific access needs or unique situations that warrant such delegation. All delegations by College Safety shall be in written form describing the specific nature of the delegated authority. College Safety will review all electronic access control delegation decisions for crime prevention and regulatory purposes.

1.3 **Installation and Modification of Electronic Access Control Doors, Cameras, Sensors, and Locking Devices:** Approved contractors (overseen by Campus Services, College Safety or ITS) are responsible for all installations or modifications of electronic access control doors, cameras, sensors, and electronic locking devices. Campus Services, along with College Safety and ITS, will develop standards, processes and procedures to ensure the consistency of electronic access control decisions made during planning, implementation, and modification of any electronic access controlled facility. These processes and procedures will address legal and regulatory requirements, crime prevention, security, safety, accountability, and adherence to appropriate campus standards while maintaining an efficient flow of traffic.

1.4 **Information Technology Services:** Information Technology Services is responsible for management and oversight of all ITS infrastructure related to electronic access control.

1.5 **Record Keeping**: College Safety is responsible for establishing and maintaining a record keeping system and operating documents required under this policy.

1.6 **Authorized Approver**: Authorized Approvers are the Deans of the relevant programs and departments, the Vice President of Instruction and Student Services or the Vice President of College Services. Faculty and staff requesting electronic card access must do so through their departments' Authorized Approver. Authorized Approvers are limited to assigned areas of responsibility. A list of Authorized Approvers will be maintained by College Safety office and updated annually.

2. Building Access

2.1 **Academic and Administrative Buildings:** With some exceptions, academic and administrative buildings are open 6:30 am to 10 pm, Monday through Friday. Weekend and holiday hours may vary dependent on building usage. After-hours electronic card access to academic and administrative buildings is limited to approved faculty, staff, and contractors with proper electronic access cards.

3. Access Card Distribution

3.1 **Faculty and Staff:** Faculty and staff needing after-hours access to locked academic, administrative and/or other buildings may be given such access through a request to their Authorized Approver. The Authorized Approver will determine the legitimacy of the need and coordinate with College Safety to enable electronic access.

3.2 **Non-CCC Individuals:** College Safety may authorize and manage the issuance of electronic access cards to non-CCC individuals in collaboration with Authorized Approvers. All access cards will be collected by Authorized Approvers upon completion of need. Authorized Approvers will notify College Safety office when access cards have been lost or not returned.

4. Master Electronic Access Cards

4.1 Requests for master electronic access cards must be submitted by an Authorized Approver to College Safety. Master access cards will only be issued if the Authorized Approver is able to demonstrate a clear business need and the request is approved by a Vice-President.

5 Sanctions for Non-Compliance

5.1 Access cards are the property of CCC and may not be retained past the date authorizing their use. In the event of a lost or unreturned access cards, the individual, the individual's department or organization may be liable for costs related to restoring security to the area.

VI. Procedure

1. Building Access Hours

1.1 General hours of operation for building access are set by College Safety, in consultation with Deans, Directors and Campus Services. If necessary, adjustments to the hours of building may be made by filing a request to your authorized approver at least 5 days in advance.

2. Faculty and Staff Access Cards

2.1 **Faculty and Staff Access:** In cases where faculty or staff need access to a locked academic, administrative or other building, the following procedures will be followed:

- The department’s Authorized Approver will determine the need for access and notify College Safety if they determine the need to be appropriate. College Safety will then update electronic access controls to allow their ID to access the building.
- Once College Safety has approved electronic access and updated access control, they will notify the Authorized Approver of the change.

2.2 **Loss of access:** Should a Faculty or Staff member lose electronic access to a building for reasons other than termination of employment, they may seek to renew their access privileges by notifying the Authorized Approver who will initiate the process for access renewal.

3. Contractors and Outside Vendors Access

3.1 **Vendor/Contractor Access:** The Authorized Approver in the department or Campus Services will review the vendor/contractor's request for access and if they determine it to be legitimate, will notify College Safety to give them necessary access.

4. Appealing Denials of Access

7.1 College Safety may deny any electronic access card request they determine to pose a security risk in all buildings. Faculty or staff denied access may contest the determination by submitting a written request to the Vice President of Instruction and Student Services or the Vice President of College Services, whose written determination will be final.

8 Internal Audit

8.1 College Safety will conduct periodic reviews of electronic access card issuance procedures to ensure that they are consistent with this policy.

VII. Related Forms

1. Electronic Access Card Request Form - use form to request electronic access card
2. Master Electronic Access Card Request Form – use form to request master electronic access card
3. Lost/Stolen Electronic Access Card Report Form – use to report lost/stolen electronic access card
4. Exception Request for Electronic Access Building Hours Form – use form to request temporary change to building unlock/lock schedule

VIII. Contacts

If you have any questions regarding this policy, please contact College Safety at (503) 594-1698 or thomas.sonoff@clackamas.edu