



## Campus Administrative Policy

**Policy Title: Access Control System**

Policy Number: 3032A

Functional Area: General Administration

---

Effective: November 1, 2025

Approved by: Terri C. Carrothers

Executive Vice Chancellor for Administration and Finance

Applies to: CU Anschutz

---

### A. Introduction

This policy applies to all buildings/sites owned or leased by the University of Colorado Anschutz Medical Campus, where the University controls access, and to all personnel assigned to work in or service University buildings. Unless otherwise stated, this policy does not extend to affiliate sites where the University of Colorado Hospital, Children’s Hospital, or other property managers control access.

### B. Table of Contents

|   |   |
|---|---|
| A. Introduction .....                                   | 1 |
| B. Table of Contents.....                               | 1 |
| C. Policy Statement.....                                | 2 |
| D. Purpose .....  | 2 |
| E. Building Access Hours.....                           | 2 |
| F. Access Control – Special Events .....                | 3 |
| G. Access Control Badge – General .....                 | 3 |
| H. Access Control Badge – Request for Access.....       | 3 |
| I. Access Control Badge – Security and Protection ..... | 5 |
| J. Access Control Badge – Design and Nomenclature ..... | 6 |

### **C. Policy Statement**

This access control policy is hereby established to preserve the personal safety of staff, students, guests, and faculty, secure the University's physical property and tangible assets, protect campus buildings from unauthorized intrusion, and protect the integrity of university research.

### **D. Purpose**

1. To limit, control, and monitor access to the University's sensitive, restricted, and controlled areas to authorized persons only.
2. To support a secure laboratory objective of controlling permitted access through a secure barrier, controlling and managing the access to areas of chemical, biological, and radioactive exposures and hazards.
3. To manage and control access to campus facilities during and after regular business hours.
4. To facilitate the identification of persons with legitimate access to and use of campus facilities, events, and programs.
5. To establish a standard process for staff, students, affiliates, contractors, guests, vendors, and faculty to obtain access to the campus and additional secured facilities areas.
6. To encourage participation in the self-policing of secure areas, controlled doors, and restricted zones.

### **E. Building Access Hours**

The University will consult with the tenants and others to establish the operating hours for the campus and each structure. Most buildings will have access control at all times.

1. Building business hours may vary depending on the work process, security needs, and public access.
2. The system always locks and alarms for all labs, high-value, high-risk, hazardous, or confidential areas.

## **F. Access Control – Special Events**

The administrator of a particular building may request or approve temporary changes to the access control protocol (hours, clearances, etc.) for special events, conferences, etc. When the building administrator approves, the Security Badging Office will adjust the programming of affected doors and alarms. Overall, building safety/security needs to be maintained during these events; security guards or police may be required at the expense of the event host.

## **G. Access Control Badge – General**

1. The University's Security Badging Office will issue all access control badges exclusively, and they will remain the property of the University.
2. The cardholder must report the loss/theft of an Access Control Badge immediately to the Security Badging Office and/or the University Police Department.
3. All University staff, contractors, students, faculty, affiliates, and others assigned to University space will obtain and display an Access Control Badge between neck and waist while in any CU Anschutz building where access is controlled.
4. The policy forbids using an Access Control Badge assigned to another person, which may result in confiscation of the badge and denial of access to both parties.
5. When a person no longer needs the Access Control Badge, i.e., termination, voluntary separation, graduation, contract completion, etc., the badge must be returned to the Badging Office. The cardholder, terminating official, or school representative should notify the Badging Office immediately so that the badge can be disabled.

## **H. Access Control Badge – Request for Access**

1. To gain access to a controlled area or building, the applicant must complete the process noted below:
  - a. Staff, Faculty, Executives, and Students, by their type of association with the University, will receive an Access

Control Badge and specific base-level access appropriate for their function or role.

- Access requests beyond the base level required by their role and employment on campus must be submitted by the Clearance Approver for the space to be accessed. The access will be granted after the Security Badging Office processes the request.
- b. Contractors and Vendors with specific purposes on campus, such as certain construction, equipment servicing, etc., may be granted time and area-limited access.
  - The designated Clearance Approver must submit requests for access
- c. University affiliates may be granted access that is consistent with their particular function and role on campus.
  - Requests for access and badging must be submitted on an Access Request Form.
  - The form requires the signature endorsement of the department administrator with whom they will be associated. Also required is a letter on the affiliate's company or hospital letterhead attesting to the validity of the request and the requesting individual's association with the sponsoring company or hospital. The Security Badging Office will grant access to controlled spaces only upon the endorsement of the authorized approver of the space for which access is sought and upon receipt of the letterhead from the applicant's home company. Expirations of these badges will be set at one year hence.
- d. The Security Badging Office will prepare periodic reports for each authorized access approver, iterating the names of those having access to the site the approver controls. The approver will correct or validate the list so it can be updated in the system.







- e. Those with multiple roles, such as student/staff, faculty/student, etc., will be issued one Access Control Badge. This badge will have the individual's required access. A non-access (PVC) card may be issued at an additional cost if a student badge is required
- f. Enrollment of other Access Control Badges from affiliates or other non-university organizations or companies will not be enrolled in the University access control system. Each independent hospital, university, company, or research complex manages its own access control risk. This policy prohibits the enrollment of CU Anschutz badges in other systems.
- g. All access control swipe data, employee information, and any biometric data is retained for six years per the University's retention policy (APS 2006).

#### **I. Access Control Badge – Security and Protection**

- 1. The security and protection of the access control badge are essential responsibilities for each cardholder. To ensure the card's continued service to the cardholder, please follow these guidelines:
  - a. Protect the card from heat and continuous exposure to direct sunlight.
  - b. Protect the card from pressure, creasing, and holes. Do not place the card in a wallet or other place where wear and abrasion will degrade the readability and function of the card
  - c. If the access control badge is lost, contact the Security Badging Office or the CU Anschutz Police Department immediately. If it is not found, the Badging Office can reissue it.
  - d. When carrying multiple access control badges, do not place them in the same carrier, as a card reader will likely be unable to read either card. Please keep them in separate carriers and separate them when presenting one to a reader.

- e. Nothing in this policy precludes charging a department/badge holder for replacing lost or damaged cards.

## **J. Access Control Badge – Design and Nomenclature**

1. The Access Control badge has several essential elements in its design:
  - a. The cardholder's photograph should reflect a current likeness. If needed, the Badging Office can update a photograph. Photo requirements include a neutral color background, an image of the cardholder's face similar to a driver's license picture, and the use of image filters that may result in the rejection of the photograph.
  - b. The cardholder's preferred name will be prominent.
  - c. The card will have a color band equivalent to the cardholder's role in the University.
    - 1) Executive\* Purple 
    - 2) Faculty Gold 
    - 3) Staff Red 
    - 4) Student Green 
    - 5) Affiliate Blue 
    - 6) Contractor/Vendor Red Hash 

These will assist in the quick recognition of the cardholder's role.

\* "Executive" is defined in Article 3 of the Laws of the Regents "Officers of the University and Administration" and listed as:

- Officers of the University
  - President;
  - University counsel;
  - Secretary of the Board of Regents;
  - Treasurer;
  - Associate vice president of internal audit
  - For the purpose of this policy, Regents would also be considered Executives

- Officers of the Administration
  - Chancellor;
  - Executive Vice Chancellor (not listed in Article 3, however, included for the purpose of this policy)
  - Vice President;
  - Associate Vice President;
  - Vice Chancellor;
  - Associate Vice Chancellor;
  - Associate Counsel;
  - Deans of the schools, colleges, and libraries.
  - Interim/acting officers are also considered officers and may receive executive access badges.
- 2. In accordance with Colorado House Bill 23-1007, the University access control card functions as the student identification card and carries Colorado Crisis Services information and Campus Crisis contact information.

## **Notes**

1. History
  - November 14, 2005: Adopted
  - December 11, 2024: Modified
  - November 1, 2025: Revised
2. Responsible Offices
  - Responsible Officer: Associate Vice Chancellor/Chief of Police
  - Prepared by: Director of Electronic Security
  - Reviewing Office: Office of the Executive Vice Chancellor for Administration and Finance