Anschutz

Campus Administrative Policy

Policy Title: Physical Security Standards

Policy Number: 3064A 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

C. Policy Statement

This physical security policy establishes construction standards to facilitate 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 establish a security standard across the campus for new construction, remodels, and infrastructure changes.

E. Security Standards

1. This policy applies to the Anschutz Medical Campus.
    a. The primary objective of CU Anschutz's physical security policies and standards is to protect people first, followed by property, research protocols, and intellectual property.
    b. When incorporated into building design, the University will benefit from the application continuity across campus.
    c. The University uses a layered approach to security. It defines this as the layers of protection and distance between the area protected and the public. This layered approach will allow controlled and permitted passage and provide a time delay, access denial, and/or physical deterrent for non-permitted entry; alarms, video surveillance, and/or data logging will monitor the effectiveness of these barriers. The

University Police Department monitors these security systems and alerts response personnel of security barriers and perimeter violations.

d. The security standards are dynamic in that they are an appropriate and timely reaction to identified risks with reasonable mitigation consistent with physical, technical, and fiscal restraints.

e. The standards support widely varied work processes, promote the fact and perception of personal security and safety, and address compliance with state, municipal, and industrial standards set in code, law, or policy.

f. Direct security costs include design/installation, procurement of components, monitoring of alarms and trouble alerts, response to alarms, periodic design review, badging, maintenance of documentation, inspections, tenant orientation, and system maintenance. Indirect security costs include the staff, training, and supplies of the Badging Office.

F. New Construction, Remodeling, and Renovation Standards

1. CU Anschutz has set construction and renovation standards in physical and electronic security to enhance the efficiency and effectiveness of new construction, renovation, relocation of offices and labs, and the integration of all work functions on campus. This document (University of Colorado, Anschutz Medical Campus, Guidelines and Design Standards) resides with the Facilities Projects Department and is distributed to all new building design teams. As projects are developed, the security requirements are incorporated into the concept designs and the commissioning of the structure. Sections 28 13 00 – Access Control and Section 08 71 00 – Door Hardware discusses current campus standards.

G. Secure Perimeters

1. All exterior doors to all buildings will have access control or door position monitoring enabled to ensure a secure perimeter of each building after the close of business.

2. The University installs access control devices at each building entrance. All buildings have at least one card-controlled door in their secure perimeter.

H. Security Installation Costs

1. The University will specify the provision of external perimeter, interior zone security, security camera coverage, alarms, panic devices, etc., consistent with the building's design, function, and current University standards. The security standards are akin to those set by the Fire Marshal, the Building Official, Information Technology, etc., wherein standards are set by a campus entity but also by one that does not fund or underwrite the project.
2. Lab managers, building administrators, research programs, specific contracts or grants, etc., may require additional security features. Security beyond the standard level requirements must be addressed by the Electronic Security Division in concert with the tenant department at the tenant's expense. Some grants and contracts may fund parts of requisite security elements. However, the tenant cannot install locking devices that prevent or impede access to law enforcement and life/safety staff. Please contact the Electronic Security Division if a tenant has additional security needs.

I. Security Cameras

1. The University uses video surveillance systems as an integral part of its physical security system. Their planned integration adds efficiency and effectiveness to the police and guard functions on the campus.
2. Cameras are typically placed on building roofs, at most building entries, at central interior junctions, and in areas of high value or high risk.
    a. Cameras are installed wherever panic alarms are installed.
    b. Cameras are installed where cash, drugs, animals, radioactive sources, and other high-risk and high-hazard areas are maintained.

c. Cameras are installed on roof parapets to continuously monitor the roof, adjacent grounds, and the portals to adjacent buildings, streets, parking areas, walkways, emergency services, etc.

d. Cameras are not placed in treatment, procedure, or other rooms where privacy is expected.

e. Cameras are installed in lobbies and entry areas so that access to elevators, stairwells, and corridors may be monitored.

3. The placement and visibility of cameras should not infer that each or any camera is monitored at all times, that a particular action or reaction may occur because of the presence of a camera, or that a camera alone adds to the security or safety of a particular area.

4. Automated License Plate Reader (ALPR)

   a. The CU Anschutz Police Department (CUPD) utilizes ALPR technology to capture and store digital license plate data and images while recognizing the established privacy rights of the public.

   b. ALPR technology allows for the automated detection of license plates. CUPD uses data associated with vehicle license plates for official law enforcement purposes, including identifying stolen or wanted vehicles, stolen license plates, and missing persons. It may also gather information about investigatory leads, and active criminal warrants. In addition, CUPD uses ALPR to detect when an excluded individual or criminal suspect arrives or has been on campus.

J. Security of Restricted Zones

1. **Physical Standards** - Security relative to research laboratories, animal colonies, and other restricted zones adjacent to public areas within the same building will have a secure perimeter. All doors to the laboratory spaces will have access control devices or will be alarmed and signed for emergency exit only. Each lab will have two secure barriers: exterior building and interior door. The

interior doors that are alarmed and controlled will remain secured at all times to ensure that only authorized personnel can enter, that a secure fire perimeter is supported, and that the line between biological, chemical, and radioactive hazards is enforced.

2. **Security Enforcement** - The integrity of the University rests with each person's commitment to support the objectives of the security system and to self-police all protected areas. This means that everyone notes doors that have been propped open, have tape across the door's strike, unescorted visitors, children in laboratory space, the wrong people in the wrong areas, intruders in offices, missing files, equipment, etc., and takes reasonable steps to remedy observations. This would include the notification of department management and/or the University Police Department. Any attempt to circumvent electronic security or to violate the Access Control policy will not be tolerated by the University. The software that controls the electronic security for campus monitors and records the status of each controlled portal.

    a. When the cause of the alarm can be attributed to an intentional act designed to circumvent the intent of the security system, the team/department/manager for the space or employee will be contacted.

    b. Absent mitigating factors that justify the security compromise, a charge for no less than $100 may be charged against the appropriate school for each violation. This charge is determined to offset the cost of dispatching the alarm, initial response and investigation, monitoring, resetting the intentional security violation, follow-up, and documentation of the violation.

    c. If the security system is damaged by intentionally circumventing the device, the school, program, or person responsible for the damage will be charged the repair cost.

K. Personal Security

1. The most valuable and irreplaceable of the University's assets is its people. The primary focus of the security standards is protecting people. To this end, each person should understand the risks before working in their particular

area, trade, function, or transiting open areas, traffic areas, etc.

2. Panic or Duress Alarms are installed in areas where a risk of robbery, confrontation, attack, or injury may occur. Typical examples are cashier offices, reception desks, drug dispensaries, etc. These areas also require security camera installation.

L. University Security Standards

1. The Director of Electronic Security and/or the Chief of Police will periodically call representatives from the various departments, schools, and divisions together to discuss trends, issues, solutions, new requirements, and concerns across campus. In addition, the Director and/or Chief will meet with representatives of the hospitals, clinics, and other tenants on campus to ensure open communication in physical, personnel, and electronic security matters.

M. Building, Department, or School Committees

1. Communication with the campus community is critical to the effectiveness of campus security. We encourage the general discussion of security concerns in each forum specific to buildings, schools, or departments with the University Police Department and/or the Electronic Security Department.

Notes

1. History
   - November 1 2025: Adopted
   - Prior to November 1, 2025, physical security standards were included in Campus Administrative Policy 3032.

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