University of Colorado Denver

Administrative Policy

Title: **Access Control and Physical Security Standards**

Source: Chancellor's Office

Prepared by: Director of Electronic Security and ID Access

Approved by: Gregory V. Stiegmann, M.D.
Interim Chancellor

Effective Date: November 14, 2005

Replaces: N/A

Applies: Anschutz Medical Campus and 9th Avenue & Colorado Campus

---

A. Introduction

This policy is applicable to all buildings/sites owned or leased for use by the University of Colorado Denver (UCD) where the University controls access and to all personnel assigned to work in or service University buildings. This policy does not extend to affiliate sites where the University of Colorado Hospital or other property managers control the access to and within their sites.

B. Table of Contents

R. Personal Security
S. University Security Committee
T. Building, Department, or School Committees

C. Policy Statement

In order to enhance and preserve the personal safety of staff, students, guests, and faculty; secure the physical property and tangible assets of the University; protect campus buildings from unauthorized intrusion; and to protect the integrity of University research, this access control policy is hereby established.

D. Purpose

1. To limit, control, and monitor access to sensitive, restricted, and controlled areas of the University to authorized persons only.

2. To support a secure laboratory objective of controlling permitted access through a secure barrier, by providing a secure fire barrier, and by controlling the areas of chemical, biological and radioactive exposures and hazards.

3. To manage and control access to campus facilities after normal business hours,

4. To facilitate, with the Access Control Badge, the identification of those persons who have 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 secured facilities or areas.

6. To encourage the participation of all in the self-policing of secure areas controlled doors, and restricted zones.

E. Building Access Hours

The University will consult among the tenants and others to establish the operating hours for each structure, however, the default unlock/relock hours are 6:00 a.m. and 6:00 p.m. during weekdays. The building's function determines whether it remains locked or is open during the workday. Some buildings will have access controlled at all times.

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. The Security Department will adjust the programming of affected doors and alarms when approved by the building administrator. Interior security for the remainder of the building or area cannot be compromised by such adjustments, so the event may have to secure police, guard services, or have to limit perimeter access.

G. Access Control Badge – General

1. All Access Control Badges will be issued exclusively by the University's Security Department Badging Offices and remain the property of the University.
2. The cardholder must report the loss/theft of an Access Control Badge immediately to the Security Department's Badging Office and the University Police Department.
3. All UCD staff, contractors, students, faculty, affiliates, and others assigned to University space, will obtain and display between neck and waist, an Access Control Badge, while on campus. In particular, the cardholder must clearly display the Access Control Badge while in secure laboratories, limited access buildings, or in other areas where all access is controlled.
4. The policy forbids the use of an Access Control Badge assigned to another person and may result in the confiscation of the badge and access denial 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 office 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 virtue of their type of association with the University, will receive an Access Control Badge and certain base level access as appropriate for their function or role.

      - Access requests beyond the base level required by their role and employment on campus, must be submitted on an Access Request Form, signed by an authorized approver for the space to be accessed. The requestor's access will be modified after the Security Department processes the request. Expirations of these badges will be set at four years hence.

   b. Contractors and Vendors, with specific purposes on campus, such as certain construction, equipment servicing, etc. may be granted time and area-limited access.

      - Requests for access and badging must be submitted on an Access Request Form. The form requires the signature endorsement of the person's sponsor, typically for the space(s) to be accessed by the person. The person's parent company will provide a letterhead document stating that the person is a representative of the company, that the company vouches for them and will vet them regarding access to sensitive areas of the campus. The Security Department will grant access to controlled spaces upon the endorsement of the authorized approver(s) of the space(s) for which access is sought. Expirations of these badges will be set at six months hence. They are renewable with validation of the required documents.

   c. Affiliates of the university may be granted access 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 which 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 his association with the

sponsoring company or hospital. The Security Department Badging Office will grant access to controlled spaces only upon the endorsement of the authorized approver(s) of the space(s) 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 Department will prepare periodic reports for each authorized approver of access iterating the names of those having access to the site the approver controls. The approver will correct or validate the list so that Security can make the corrections to the access control system.

e. Those with multiple roles, such as student/staff; faculty/student, etc. will be issued no more than two Access Control Badges, each with a role specific badge presentation with the title, school, or function noted on the card face. Access clearances required for each role will be specific to the role and may be time/day limited, as required by the area restrictions. Each may have different expiration schedules assigned to them.

f. Enrollment of other Access Control Badges – Access Control Badges from affiliates or other non-UCD organizations or companies will not be enrolled in the UCD access control system. Each independent hospital, university, company, or research complex manages its own access control risk. This policy prohibits enrolling UCD badges in other systems.

I. Access Control Badge – Security and Protection

1. The security and protection of the access control badge are important responsibilities for each cardholder. The badge cost, processing labor, printing, and tracking, assign a significant value to each badge. Each card has a loop antenna embedded in it that communicates a unique signal to the card reader. The card is expensive and carelessness creates an unnecessary impact to University funds. 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 lost, contact one of the Security Department's Badging Offices immediately. If not found, the Badging Office can reissue the access control badge. Also, advise the University Police Department of its loss or theft. Nothing in this policy precludes the recharging to the department $15 for the replacement of cards that are lost or damaged due to negligence.

   d. When carrying multiple access control badges, do not place them in the same carrier, as a card reader will likely not be able to read either card. Keep them in separate carriers and separate them when presenting one to a proximity reader. When in UCD space displays the appropriate badge on top for the space being accessed.

J. Access Control Badge – Design and Nomenclature

1. The Access Control badge has a number of important elements in its design:

   a. The cardholder's photograph should reflect a current likeness. If needed, the Badging Office can update a photograph. The new template provides a white background to the cardholder's face.

   b. The library barcode allows the card to function as a University library card.

   c. The cardholder's preferred name will be prominent. Middle initials and generational suffixes are allowed.

   d. The cardholder's academic and professional credentials may follow the surname, i.e. MD, PhD, RLATG, MS, CPP, RN, MPA, MCJ, BA, etc.

   e. The cardholder's title, program, or department and school or division will be beneath the cardholder's name.

   f. The cardholder's division, company, hospital etc. such as Central Services and Administration, University of Colorado Hospital, will appear on the third line.

   g. The expiration date of the card will denote the date that the card and its associated access privileges will expire. The cardholder should initiate renewal requests for extended access 30 days before expiration.

   h. The card will have a color band equivalent to the cardholder's role in the University. These will assist in the quick recognition of the cardholder.

      - Executive Purple
      - Faculty Gold
      - Staff Red
      - Student Green
      - Affiliate Blue
      - Contractor/Vendor Red Hash

   i. The Badging Office will print on both sides of the Access Control Badge so that the photo and data will always be visible.

K. Security Standards

1. This policy applies to the Anschutz Medical Campus and the 9th Avenue & Colorado campus:

   a. The primary objective of UCD physical security policies and standards are to protect people first, with property, research protocols, and intellectual property behind it.

b. When incorporated into building design, the University will enjoy a continuity of application between each building and each zone. Architectural considerations for the presentation of buildings should incorporate these standards and those in the current CSI Division 16722 statement as representative of the University's security position.

c. The University uses a layered approach to security provision. It defines this as the provision of barriers and distance between the area protected and public areas, with security provided to and around the object of protection first and then working outward with additional layers, as needed. Barriers will allow controlled and permitted passage but will also provide a time delay, access denial and/or physical deterrent for non-permitted entry. Alarms, CCTV surveillance, and/or data logging by the Security Department monitor the effectiveness of these barriers. The University Police Department also monitors these barriers by foot and vehicle patrol. The security system alerts response personnel from the University Police Department of violations to the various security barriers and perimeters. The greater the value or risk of the protected area, the greater and more complex the perimeter and barrier protection.

d. The security standards are dynamic in that they are an appropriate and timely reaction to identified risks with reasonable mitigation to those risks, consistent with physical, technical, and fiscal restraints. As the risk changes, the associated security model will react and change appropriately.

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

f. The costs of security include the cost of 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 costs of security include the monitoring staff, the Badging Offices staff, training, and supplies.

L. New Construction, Remodeling, and Renovation Standards

1. UCD has set construction and renovation standards in the areas of 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 both campuses. This document (CSI Division 16722) 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 through to commissioning of the structure.

M. Hours of Operation

1. The standard and default hours of operation for the security of exterior entrance doors are from 6:00 a.m. to 6:00 p.m. Perimeter door alarms are also linked to the default time specification. Those enrolled in the Access Control System will be able to enter any access-controlled door for which after-hours access has been granted to that cardholder. The main entrances to most buildings will be unlocked and publicly accessible during the weekday/daytime hours. The security system locks and alarms for all labs, high-value, high-risk, hazardous, or confidential areas are armed at all times. Business hours for some

buildings may vary depending upon the work process, security needs, and public access.

N. Secure Perimeters

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

2. The University installs access control devices at a building's primary entrance(s), where the area secured must limit access to a large and variable population, where the contents of the area present a high value or a high risk of injury; where after-hours access must be logged, and/or where unique circumstances require monitored access control. All buildings will have, by default, at least one card controlled door in its secure perimeter.

O. Security Installation Costs

1. The University will specify the provision of external perimeter, interior zone security, CCTV coverage, alarms, panic devices, etc. consistent with the design of the building, its function, and the current University standards. The security standards are akin to the standards 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, certain contracts or grants, etc. may request security features or elements beyond that required by these standards. Security beyond the standard level requirements must be addressed by the Security Department in concert with the tenant department, generally, at the expense of the tenant. Some grants and contracts may fund parts of requisite security elements. However, the tenant is not at liberty to install locking devices that prevent or impede access to law enforcement and life/safety staffs. Should a tenant have additional security needs, the Security Department will be contacted so that those specific needs can be addressed, coordinated with the University system, and with customer satisfaction ensured.

P. Closed Circuit Television (CCTV)

1. The University uses CCTV systems as an integral part of its physical security system. Their efficient integration adds efficiency and effectiveness to the police and guard functions on the campuses.

2. Cameras are typically placed on building roofs, at most staff, student and public building entries, at central interior junctions, and in areas of high value or high risk.

   - Cameras are installed wherever panic alarms are installed.

   - Cameras are installed in areas where cash, drugs, animals, radioactive sources and other high-risk and high-hazard areas are maintained.

   - Cameras are installed on roof parapets for continual surveillance of the roof, adjacent grounds, the portals to adjacent buildings, streets, parking areas, walkways, emergency services, etc.

- Cameras are not placed in clinic, treatment, procedure, or other rooms where there is an expectation of privacy.

- Cameras are installed in ground level lobbies and entries such that access to elevators, stairwells, corridors may be recorded.

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 take place because of the presence of a camera, or that a camera, by itself adds to the security or safety of a particular area.

Q. Security of Restricted Zones

Physical Standards - Security relative to research laboratories, animal colonies, and other restricted zones adjacent to public areas within the same building will have 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: the building exterior and an interior door system. 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. The Security Department, the Fire/Safety Office, and the Environmental Health & Safety Department have an interest in the security of the laboratory perimeter.

Security Enforcement - The integrity and value of the University rests with the individual commitment of each person 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, and 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 further include the notification of department management, the Security Department and/or the University Police Department. Any attempt to circumvent the electronic security or to violate the Access Control policy cannot be tolerated by the University. The software that controls the electronic security for both campuses monitors and records the status of each controlled portal.

- When the cause of the alarm can be attributed to an intentional act designed to circumvent the intent of the security system, the Dean of the appropriate school will be notified by the Chief of Police and will have five days to provide to the Chief of Police mitigating factors, if any, for the security compromise.

- At the end of the five-day period, the Chief of Police will consider mitigation, if any, submitted toward the resolution of the violation.

- Absent mitigating factors that justify, in the opinion of the Chief of Police, the security compromise, a charge of an amount no less than $100 will be recharged against the appropriate school for each violation. This charge is determined to offset the cost of the dispatching of the alarm, initial police response and investigation, monitoring and resetting of the intentional security violation, follow up by the Chief of Police and the need to track the violation.

- In the event that the security system sustained damage from the intentional act to

circumvent the device, the cost of repair will be recharged to the school or program if more than $100.

R. Personal Security

1. The most valuable and irreplaceable of the University's assets is its people. The primary focus of the security standards is the protection of people. To this end, each person should understand the risks before them when working in their particular area, trade, or function; when transiting open areas, traffic areas, etc. At each primary door entry and in all parking areas, "Code Blue" pylons have been installed. Each of these provides direct 9-1-1 access to the Police Dispatcher and are operable at all times.

2. Panic or Duress Alarms are installed in areas where a risk of robbery, confrontation, attack, or injury may occur. Typical of these would be cashier offices, reception desks, drug dispensaries, etc. These areas are also typically supported by CCTV installation.

S. University Security Committee

1. The University will form a Security Committee to address security issues within the University setting as well as the campus settings, as necessary. Representatives from the various departments, schools, and divisions will be called together periodically by the Director of the Electronic Security Department to discuss trends, issues, requirements, and solutions. The committee will also expand periodically to include representatives of other hospitals, clinics, and tenants on the campuses to ensure open communication in areas of physical, personnel, and electronic security.

T. Building, Department, or School Committees

1. Communication with the campus community is critical to the effectiveness of security on the campuses. 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.