



Original Approval Date: June 27, 2005
Most Recent Approval: November 1, 2019
Editorial Amendments: March 16, 2026

Parent Policy: [Lands and Buildings Security Policy](#)

Access Control Security Systems on Urban Campus Areas Procedure

Office of Administrative Responsibility:	Campus Operations and Services University of Alberta Protective Services
Approving Authority:	Vice-President (University Services, Operations and Finance)

Purpose

The University of Alberta strives to provide a safe, comfortable, secure environment while minimizing instances of theft or damage of equipment, furniture and other property. The university will outline responsibilities for installation, maintenance, and monitoring of access control and security systems and response to alarms, as well as the assignment of costs associated with each, to ensure consistency and effectiveness in an efficient and economical manner.

The University recognizes that Urban Campus Areas are vastly different in population, use and management than University Owned and Leased Rural Lands and that the management of safety and security on these properties may differ. This policy document applies only to university owned, leased, rented or controlled lands, buildings and residences on Urban Campus Areas.

The purpose of this policy document is to:

- Identify the process for requesting a security assessment;
- Identify the process for installing an access control, security, and video monitoring system;
- Identify the responsibilities for granting access privileges;
- Identify who is responsible for costs associated with the installation, maintenance and monitoring of access control security, and video monitoring systems;
- Identify centrally supported services vs. services paid for by user groups;

- Identify a budget pricing guide;
- identify security solutions available to faculties, facilities and external consultants; and
- Identify procedures for viewing video, security and card access system logs.

Definitions

The attached definitions table outlines the terms used in this policy document and any specific rules of interpretation that apply.

Scope

Compliance with this policy document extends to all academic, support and excluded staff, postdoctoral scholars, and academic colleagues as outlined and defined in the *Recruitment Policy*; undergraduate, graduate students and post-graduate learners; emeriti; members of the Board of Governors; visitors to campus, including visiting speakers and scholars; third party contractors / consultants; and volunteers.

Procedure

[SECURITY ASSESSMENT](#)

[INSTALLATION OF SYSTEMS](#)

[ACCESS PRIVILEGES](#)

[COST RESPONSIBILITIES](#)

[REQUESTS TO VIEW VIDEO OR SECURITY AND ACCESS LOGS](#)

SECURITY ASSESSMENT

1. CRIME PREVENTIONS THROUGH ENVIRONMENTAL DESIGN (CPTED)
 - a. All faculties, departments and units must consult with University of Alberta Protective Services (UAPS) if they are considering the installation of, modification or expansion of existing security, card access and video monitoring systems within their assigned space(s), by requesting a CPTED review. UAPS will only be responsible for monitoring and responding to Protective Services approved security related alarms, and must be involved in the selection, design and implementation of all security systems. This applies to intrusion alarm systems, card access, video monitoring and any other security related monitoring and alarm systems. UAPS will work with the faculty, department, or unit, in conjunction with Facilities and Operations (F&O) to determine the appropriate security solution.

INSTALLATION OF SYSTEMS

2. SECURITY SYSTEMS
 - a. Security Systems, also called Intrusion Systems, are equivalent to residential Burglary

Alarm Systems. Alarms from security systems are centrally monitored and responded to by UAPS.

- b. Either F&O University Trades will do installation of security systems, or an F&O approved and contracted third party contractor. Faculties, departments and units may not contract the work themselves.
- c. All security system implementations on all campuses shall be based upon standard systems centrally supported by F&O and will operate on the F&O FMNet network.
- d. All security system implementations on all campuses will include at least one (1) camera, viewable only by UAPS to provide appropriate response to alarms.
- e. F&O manages Security Systems and is responsible for:
 - i. the database associated with the security system;
 - ii. for granting access privileges to central support units such as UAPS, Environmental Health, Safety and Environment (HSE), trades and building services, where necessary;
 - iii. for providing detailed requirements for ACS design;
 - iv. for interfacing with Faculty-based Access Control Administrators (FACA);
 - v. F&O maintains the passwords and passcodes for each individual enrolled as requested by the Faculty, Department or unit assigned FACA(s). Passcodes are created by F&O and are unique to each individual. Passcodes and passwords are shared only with the individual.
- f. Faculties, departments and units are responsible for learning how to use the security system and for:
 - i. Assigning a Facility Access Control Administrator(s) (FACA) to provide administrative support for their assigned space(s).
 - 1. FACA's are responsible for initial and ongoing management of user assignment for their area(s) of responsibility
 - 2. Manuals will be provided by F&O. Training will be provided upon request.
- g. Standalone security systems are not permitted.

3. ACCESS CONTROL SYSTEMS (ACS)

- a. Standard practice is to install keyed locks to secure doors. Faculties, Departments and units may request convenience access control for doors within their assigned space.
 - i. Convenience Access Control doors are not monitored for alarms.
 - ii. Where alarms are required to be monitored a Security System will be considered instead.

- b. All access control implementations on all campuses are based upon standard centralized systems supported by F&O, and will operate on the Facilities and Operations FMNet network.
- c. F&O manages Access Control and is responsible for:
 - i. the database associated with the access control system doors;
 - ii. for granting access privileges to central support units such as UAPS, Environmental Health and Safety (EH&S), trades and building services;
 - iii. for providing detailed requirements for ACS design; and
 - iv. for interfacing with Faculty-based Access Control Administrators (FACA).
- d. Faculties, departments and units are responsible for learning how to use the access control system and for:
 - i. Assigning a FACA to provide administrative support for their assigned space(s);
 - 1. FACA's are responsible for initial and ongoing management of card access assignment for their area(s) of responsibility
 - 2. Where multiple Faculties, departments and units occupy a building, assignment of access into common areas will overlap.
 - 3. Manuals will be provided by F&O. Training will be provided upon request.
- e. Standalone access control systems are not permitted.

4. VIDEO MONITORING SYSTEMS

- a. Video monitoring systems as they pertain to security will adhere to the *Video Monitoring Procedure* and *Protection of Privacy Act (POPA)* requirements as provided by the Information, Privacy and Records Management Office (IPRMO).
- b. Faculties, Departments and units must apply to UAPS for video monitoring approval following the recommendations of the associated CPTED report.
- c. All security system implementations on all campuses will include at least one (1) camera, viewable only by UAPS to provide appropriate response to alarms.
- d. Either F&O University Trades, or an F&O approved and contracted third-party contractor, will install video monitoring systems. Faculties, departments and units may not contract the work themselves.
- e. All video monitoring system implementations on all campuses shall be based upon standard systems centrally supported by F&O and will operate on the F&O FMNet network.
- f. Video recording is maintained by F&O and is only accessible to UAPS for investigative and alarm response purposes. Cameras are not actively monitored and are not used to

monitor individual performance. Recorded video will only be shared with Faculties, Departments and units at the discretion of UAPS based upon their investigation.

- g. Standalone video monitoring systems for security purposes are not permitted.
- h. All video monitoring to be installed or currently in place, regardless of purpose and intent, must be declared and vetted by UAPS in accordance with the *Video Monitoring Procedure* and *Protection of Privacy Act* requirements as provided by IPRMO.

ACCESS PRIVILEGES

5. SECURITY SYSTEMS

- a. F&O: F&O maintains the passwords and passcodes for each individual enrolled as requested by the faculty, department or unit assigned FACA(s). Passcodes are created by F&O and are unique to each individual. Passcodes and passwords are shared only with the individual.
- b. The respective FACA is responsible for requesting passcode assignments for their staff and students for their area of responsibility. They are responsible for keeping track of who has access to their area(s) as well as updating/confirming Emergency Contact information to ensure that it is kept current. Intrusion Contact Information Forms found under the Forms section of this procedure are to be provided to F&O.

6. ACCESS CONTROL SYSTEMS

- a. Exterior / Perimeter / Common Area Access Control
 - i. F&O: Building exteriors/perimeters and common areas are the responsibility of F&O to maintain. F&O is responsible for assigning access privileges to central support units such as Protective Services, EH&S, trades and building services.
 - ii. FACA: is responsible for assigning access privileges to the perimeter / common area doors for their staff and students. The number of exterior doors to be accessible after hours will be limited.
- b. Interior Faculty, Department and Unit Door Access Control
 - i. F&O: responsible for assigning access privileges to central support units such as UAPS, HSE, trades and building services.
 - ii. FACA: responsible for assigning access privileges to the interior doors for their staff and students.
 - iii. Restricted access areas are to have signage on doors identifying the hazards present along with a 24 hour x 365 day number to call to obtain access.
- c. Lost/Stolen Keys and Cards

- i. Users must report such incidents to their Faculty or department immediately. The faculty or department is responsible for removing all access privileges from the lost or stolen card and reporting the lost/stolen cards and keys to F&O.
- ii. ONEcard's Lost/Stolen Card Website is not linked to the F&O's central system and only affects ONEcard services such as Meal Plans, printing services, etc.

COST RESPONSIBILITIES

7. CAPITAL CONSTRUCTION / MAJOR RENOVATIONS

a. Central Infrastructure

- i. Costs for the central infrastructure for Security, Access Control and Video Monitoring are to be borne by the Construction project for infrastructure required to be physically installed in the building.
- ii. Central Infrastructure includes:
 1. Network (FMnet): Network Switch, Fiber, UPS, Data Cabling, Racks, etc.
 2. Security Systems: To be determined during design.
 3. Access Control System: Controllers, Boards, Cabling, Readers (Exterior and Common Area doors), Power Supplies, etc.
 4. Video Monitoring System: Where deemed necessary by F&O a Video Recorder, supplied and installed by F&O, maybe required.

b. Tenant Fit-up

- i. Costs for tenant fit-up for Security, Access Control and Video Monitoring are to be borne by the Construction project for equipment required to be physically installed in the tenant space.
- ii. Tenant Fit-up Infrastructure includes:
 1. Network (FMnet): To be determined based on Fit-up requirements for Security, Access Control and Video Surveillance/Monitoring systems.
 2. Security Systems: Controllers, Boards, Sensors, Keypads, Cabling, etc.
 3. Access Control System: Readers (Interior doors), Cabling, Power Supplies (where necessary), etc.
 4. Video Monitoring System: Cameras.

8. SMALL RENOVATIONS / INSTALLATIONS

a. Infrastructure

- i. Network: For most existing buildings the network infrastructure already exists. Where additional network infrastructure may be required to accommodate a new installation F&O will assess the need and responsibility for costs will be addressed on a per project basis.
- ii. Security Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.
- iii. Access Control Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.
- iv. Video Monitoring Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.

9. EXPANSION / UPGRADING / MAINTENANCE

a. Central Infrastructure

- i. F&O is responsible for the costs associated with maintaining and updating software and firmware of all Network, Security, Access Control and Video Monitoring central equipment infrastructure.
- ii. F&O may determine that expansion or upgrading Network, Access Control or Video Monitoring System infrastructure is necessary to provide better service to the end user. In such cases the cost responsibility will be determined during budgeting.

b. Security Systems

- i. Faculties and Departments are responsible for the costs associated with maintaining security systems installed within their area(s).
- ii. Existing Security Systems which communicate over telephone lines are to be updated with a network connection. The cost of the network card and cabling is the responsibility of the Faculty or Department.
 - 1. Where the existing system does not already have video monitoring, at least one (1) camera must be installed. The cost of the cable and camera(s) is the responsibility of the Faculty or Department.
- iii. Existing Security Systems which are no longer supported by F&O: the cost to upgrade to a new security system with a network connection is the responsibility of the Faculty or Department.
 - 1. F&O will provide reasonable notice to Faculties, Departments and units to allow for budget planning.
 - 2. Faculties, Departments and units who do not upgrade their Security System will risk losing alarm monitoring and response by UAPS.
 - 3. Additionally, the existing security system will be disconnected and

removed at the cost of the Faculty, department or unit as standalone systems are not permitted.

c. Access Control Systems

- i. Exterior / Perimeter / Common Area Access Control: F&O is responsible for the maintenance of all Exterior / Perimeter / Common Area doors.
- ii. Interior Faculty, Department and Unit doors: faculties and departments are responsible for the costs associated with maintaining interior doors.

d. Access Control Cards and Keys

- i. Faculties and users are responsible for costs associated with lost, stolen or damaged ONEcards and Generic cards.
- ii. Faculties and users are responsible for costs associated with lost, stolen, broken or damaged keys as outlined in the *Lock Changes, Key Request and Key Control Procedure*.

e. Video Monitoring Systems: Faculties and Departments are responsible for the costs associated with maintaining cameras. F&O will notify the faculty or department when there is an issue with any cameras that require a service call.

f. Refer to the *Security Services Matrix* for further information on responsibilities and costs associated with different types of security systems available.

REQUESTS TO VIEW VIDEO OR SECURITY AND ACCESS LOGS

10. SECURITY AND CARD ACCESS SYSTEM LOGS

- a. Requests for logs must come through UAPS as part of an investigation.
- b. Requests for logs for time and attendance tracking must come from Central Human Resources if the request is not part of a UAPS investigation.
- c. Requests to F&O from faculties, departments and units will not be considered.

11. VIDEO MONITORING

a. Live Monitoring

- i. Live monitoring of video is only available to UAPS unless operational permissions are provided to specific users by UAPS via the *Video Monitoring Procedure* and configured in the central infrastructure systems by F&O.
- ii. Video cameras are not actively monitored by UAPS and are used to investigate reported incidents and for use in determining the best response to security alarms and events.

b. Recorded Video

- i. Recorded video is only available to UAPS;
 - ii. Requests to F&O from faculties, departments and units will not be considered.
 - iii. Recorded video may be shared with faculties, departments and units at the discretion of UAPS as part of an investigation.
- c. Refer to the *Security Services Matrix* for further information on responsibilities and estimated costs associated with different types of security systems available.

Security Services Guidelines & Matrix - November 1, 2019

A security matrix was developed to provide a guideline of security services available to assist faculties, Departments and external project consultants identify solutions available for implementation within the University of Alberta environment.

The matrix identifies four risk levels: low, medium, high and ultra. The use of these definitions provides guidance for the minimum level of security to be maintained within a facility.

Certain locations have specific entry procedures to ensure the safety of the security response team. These detailed procedures ensure the protection of people, assets within the space, and data stored within the premises.

Increased security measures within a protected space have incremental cost factors for initial installation, ongoing lifecycle maintenance costs and an anticipated accrual fee for renewal. These cost estimates are captured in the security matrix. The University is not funded for increased operational security requirements being requested by faculties and departments. These enhanced services come with an installation and service fee, which is in line with external industry standards, and are outlined in the matrix.

Traditional Keys:

The basic key system used on campus is provided by Facilities & Operations. This is the minimum level of protection required for any campus facility. As indicated by the Lock Changes, Key Request and Key Control Procedure, faculties and Department administer and maintain records of key holders and authorize the issuance of additional keys. This affords maximum flexibility to the faculties and departments, however minimizes the actual security protection offered. The maintenance of accurate records by the faculties and departments establishes the true level of security for a facility. The initial implementation of a traditional key system is supported infrastructure.

High Security Keys:

A high security key provides an additional level of protection in the fact that the cylinder core (keyway) of the lock contains anti-picking features over standard issue cores.

The Facilities and Operations Lock Shop maintains control of issuing and documenting keys. Issuing and documenting access to keys improves the overall security measures effectiveness for a facility.

Master Key Override:

Master keys have limited distribution within the campus. These keys are distributed to security response forces, key facility maintenance and faculty and department administrators. The loss of this type of key will require all doors controlled by the override key to be re-keyed. This represents a significant cost to the person or group that lost the key.

Convenience Card Access (On line-local alarm – no response):

This is an on-line card reader that reports real time security events. It represents the first level of electronic security and forms the basic building block to increase the security protection level. This basic installation allows time zones to be established when a specific door will remain locked or unlocked and reports the status of a door, open or closed. The reader contains a small buzzer that will activate when a door is propped or held open. Lost and stolen cards are removed from the system upon reporting the loss to faculty, department or facility administrator. Facilities and Operations will administer access control privileges through a web browser security interface for exterior access controlled doors.

PIN/Keypad Card Readers:

This is the same as the card reader above with the addition of a key pad added to the front of the card reader. Entry into this type of secured premises will require the entry of a user definable pin number into the keypad along with presentation of the card. This reduces the likelihood that a lost card can be used to gain entry into protected premises.

Intrusion Alarm Security Systems:

This is best described as a commercial grade home intrusion burglar system. It utilizes phone lines or Ethernet for dialing and connecting to UAPS to inform them of an intrusion. It utilizes a keypad to arm and disarm an alarm detector in the protected space. All intrusion alarm security systems must include the installation of a video surveillance monitoring camera for UAPS to monitor and respond to alarms.

Biometrics:

Biometric devices are available for securing high level and ultra secure facilities. Costs are not shown as the type of biometric device chosen can significantly impact the cost.

Elevator Control:

Elevator control is often used to provide a security solution for open building concept construction. Elevator control is costly in nature and requires extensive administration to effectively secure premises. The concept of tailgating or hitching a ride to a secure floor is prevalent. Thought should be given towards securing a building floor plate over employing elevator control to manage a secure environment.

Budget Pricing:

The following budget guidelines and the security matrix are provided for information purposes when planning construction activities that may include card access controlled

doors, remote monitoring, intrusion alarms or other security features.

Budget Pricing Guidelines:

1. Budget pricing guidelines for design purposes: (2019 estimated Canadian dollars)

- a. \$6,000 per Access Control System (ACS) door with card access control (i.e. door with a card reader and electric lock)
- b. \$5,500 per ACS door that is electrically controlled, but without a card reader
- c. \$1,500 per door that is only roughed in for potential future ACS installation
- d. \$5,000 per elevator requiring floor selective ACS
- e. \$2,000 per floor for an elevator requiring a 'Hall Call' ACS reader on each floor
- f. \$3,500 per video camera
- g. \$32,000 per intrusion alarm security system
- h. These above are guidelines only. Features, site conditions, equipment locations, etc. will dictate actual costs. Ensure that budget estimates are updated regularly during the design process. Contact Campus Operations and Services for current cost estimates.

2. Facilities and Operations can assist faculties, departments and units in developing their budgets for ongoing security system repair, maintenance and database administration.

3. Faculties and users are responsible for costs associated with lost, stolen, broken or damaged keys. Please refer to the *Lock Changes, Key Request and Key Control Procedure*.

Definitions

<i>Any definitions listed here apply to this policy document only with no implied or intended institution-wide use. For clarity, defined terms listed here include grammatical variations thereof.</i>	
University Owned and Leased Rural Lands	University owned and leased rural lands are large rural land blocks owned or leased by the University. University rural lands follow the municipal zoning for agriculture use with a minimum clearance of one mile of a fringe area as defined in the municipal policies for Edmonton, St Albert, Morinville, Camrose, Calgary and other urban centres.
Urban Campus Areas	Urban campus areas include all University property located within a municipal zone (i.e. Edmonton, Calgary, Camrose) and any land owned within one mile of a fringe area as defined in the municipal policies for Edmonton, St. Albert, Morinville, Camrose, Calgary and other urban centres.

Parent Policy Suite

- [Lands and Buildings Security Policy](#)
- [Access Control Security Systems on Urban Campus Areas Procedure](#)
- [Building Hours of Operation Procedure](#)

- [Control Centre Alarm Monitoring and Response Procedure](#)
- [Lock Changes, Key Request, and Key Control Procedure](#)
- [Request for Access to Utility Service Corridors Procedure](#)
- [Video Monitoring Procedure](#)

Related Policy Documents

- There are no related policy documents.

Related Links

- [Access Control Security Systems Security Services Matrix](#)
- [Campus Operations and Services](#)
- [Information, Privacy and Records Management Office](#)
- [Protective Services \(UAPS\)](#)

History

- June 27, 2005 Approved.
- November 1, 2019 Approved.
- March 16, 2026 Editorial amendment. Formatting, office name and links.

*For questions surrounding policy document interpretation or implementation,
please contact the Office of Administrative Responsibility.*

The official version of this document may be obtained from <https://www.ualberta.ca/policies-procedures/index.html>