Original Approval Date: June 27, 2005

Most Recent Update: November 1, 2019

Parent Policy: Lands and Buildings Security Policy

Access Control/Security Systems on Urban Campus Areas Procedure

Office of Administrative Responsibility:	Operations & Maintenance (Facilities & Operations) University of Alberta Protective Services (Risk Management Services)
Approver:	Vice-President (Facilities & Operations) Vice-President (Finance & Administration)
Scope:	Compliance with this University policy extends to all academic, support and excluded staff, postdoctoral fellows, and academic colleagues as outlined and defined in the Recruitment Policy (Appendix A and Appendix B: Definitions and Categories), undergraduate, graduate, Faculty of Extension students, emeriti, members of the Board of Governors, visitors to campus, visiting speakers and scholars, third party contactors and volunteers.

Overview

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 procedure applies only to University owned, leased, rented or controlled lands, buildings and residences on urban campus areas.

Purpose

This procedure will:

- 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
- Identify procedures for viewing video, security and card access system logs

PROCEDURE

SECURITY ASSESSMENT

1. CRIME PREVENTIONS THROUGH ENVIRONMENTAL DESIGN (CPTED)

   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. Protective Services will only be responsible for monitoring and responding to Protective Services approved security related alarm, 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. Protective Services will work with the faculty, department, or unit, in conjunction with Facilities & Operations (F&O), to determine the appropriate security solution.

INSTALLATION OF SYSTEMS

2. SECURITY SYSTEMS

   Security Systems, also called Intrusion Systems, are equivalent to residential Burglary Alarm Systems. Alarms from security systems are centrally monitored and responded to by University of Alberta Protective Services (UAPS).

   Either Facilities & Operations (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.

   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.

   All security system implementations on all campuses will include at least one (1) camera, viewable only by UAPS to provide appropriate response to alarms.

   F&O manages Security Systems and is responsible for:
   a. The database associated with the security system;
   b. For granting access privileges to central support units such as UAPS, Environmental Health and Safety (EH&S), trades and building services, where necessary;
   c. For providing detailed requirements for ACS design;
   d. For interfacing with Faculty-based Access Control Administrators (FACA);
   e. 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.

   Faculties, departments and units are responsible for learning how to use the security system and for:
   a. Assigning a Facility Access Control Administrator(s) (FACA) to provide administrative support for their assigned space(s);
      i. FACA's are responsible for initial and ongoing management of user assignment for their area(s) of responsibility
      ii. Manuals will be provided by F&O. Training will be provided upon request.

   Standalone security systems are not permitted.

3. ACCESS CONTROL SYSTEMS (ACS)

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

a. Convenience Access Control doors are not monitored for alarms.
b. Where alarms are required to be monitored a Security System will be considered instead.

All access control implementations on all campuses are based upon a standard centralized systems supported by F&O, and will operate on the Facilities and Operations FMNet network.

F&O manages Access Control and is responsible for:

a. The database associated with the access control system doors;
b. For granting access privileges to central support units such as UAPS, Environmental Health and Safety (EH&S), trades and building services;
c. For providing detailed requirements for ACS design;
d. And for interfacing with Faculty-based Access Control Administrators (FACA).

Faculties, departments and units are responsible for learning how to use the access control system and for:

a. Assigning a Facility Access Control Administrator(s) (FACA) to provide administrative support for their assigned space(s);
    a. FACA's are responsible for initial and ongoing management of card access assignment for their area(s) of responsibility
    b. Where multiple Faculties, departments and units occupy a building, assignment of access into common areas will overlap.
    c. Manuals will be provided by F&O. Training will be provided upon request.

Standalone access control systems are not permitted.

VIDEO MONITORING SYSTEMS

Video monitoring systems as they pertain to security will adhere to the Video Monitoring Procedure (UAPPOL) and Freedom of Information and Protection of Privacy (FOIPP) guidelines posted by the Information and Privacy Office (IPO).

Faculties, Departments and units must apply to UAPS for video monitoring approval following the recommendations of the associated CPTED report.

All security system implementations on all campuses will include at least one (1) camera, viewable only by UAPS to provide appropriate response to alarms.

Either Facilities & Operations University Trades will install installation of video monitoring systems, or an F&O approved and contracted third party contractor. Faculties, departments and units may not contract the work themselves.

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.

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.

Standalone video monitoring systems for security purposes are not permitted.

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 (UAPPOL) and Freedom of Information and Protection of Privacy (FOIPP) guidelines posted by the Information and Privacy Office (IPO).

ACCESS PRIVILEGES

1. SECURITY SYSTEMS

   Facilities and Operations (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.

   The respective Facility Access Control Administrator (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.

2. ACCESS CONTROL SYSTEMS

   a. Exterior / Perimeter / Common Area Access Control

      a. Facilities and Operations (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.

      b. Facility Access Control Administrator (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

      a. Facilities and Operations (F&O) is responsible for assigning access privileges to central support units such as Protective Services, EH&S, trades and building services.

      b. Facility Access Control Administrators (FACA) are responsible for assigning access privileges to the interior doors for their staff and students.

      c. 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

      a. 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.

      b. 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

1. CAPITAL CONSTRUCTION / MAJOR RENOVATIONS
    a. Central Infrastructure
        a. Costs for the cental 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.
        b. Central Infrastructure includes:
            a. Network (FMnet): Network Switch, Fiber, UPS, Data Cabling, Racks, etc.
            b. Security Systems: To be determined during design.
            c. Access Control System: Controllers, Boards, Cabling, Readers (Exterior and Common Area doors), Power Supplies, etc.
            d. Video Monitoring System: Where deemed necessary by F&O a Video Recorder, supplied and installed by F&O, maybe required.
    b. Tenant Fit-up
        a. 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.
        b. Tenant Fit-up Infrastructure includes:
            a. Network (FMnet): To be determined based on Fit-up requirements for Security, Access Control and Video Surveillance/Monitoring systems.
            b. Security Systems: Controllers, Boards, Sensors, Keypads, Cabling, etc.
            c. Access Control System: Readers (Interior doors), Cabling, Power Supplies (where necessary), etc.
            d. Video Monitoring System: Cameras.

2. SMALL RENOVATIONS / INSTALLATIONS
    a. Infrastructure
        a. Network: For most existing buildings the network infrastructure already exists. Where additional network infrastructure maybe required to accommodate a new installation F&O will assess the need and responsibility for costs will be addressed on a per project basis.
        b. Security Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.
        c. Access Control Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.
        d. Video Monitoring Systems: The cost of new installations, additions or modification to an existing system is the responsibility of the project.

3. EXPANSION / UPGRADING / MAINTENANCE
    a. Central Infrastructure
        a. 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.
        b. 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
        a. Faculties and Departments are responsible for the costs associated with maintaining security systems installed within their area(s).
        b. 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.
            a. 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.
        c. 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.
            a. F&O will provide reasonable notice to Faculties, Departments and units to allow for budget planning.
            b. Faculties, Departments and units who do not upgrade their Security System will risk losing alarm monitoring and response by UAPS.
            c. 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
        a. Exterior / Perimeter / Common Area Access Control
            a. F&O is responsible for the maintenance of all Exterior / Perimeter / Common Area doors.
        b. Interior Faculty, Department and Unit doors
            a. Faculties and Departments are responsible for the costs associated with maintaining interior doors.
    d. Access Control Cards and Keys
        a. Faculties and users are responsible for costs associated with lost, stolen or damaged ONEcards and Generic cards.
        b. 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

a. 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 requires a service call.

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

REQUESTS TO VIEW VIDEO OR SECURITY AND ACCESS LOGS

1. 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 Facilities and Operations (F&O) from Faculties, Departments and Units will not be considered.

2. VIDEO MONITORING
   a. Live Monitoring
      a. Live monitoring of video is only available to UAPS unless operational permissions are provided to specific users by UAPS via the Video Monitoring Procedures and configured in the central infrastructure systems by F&O.
      b. 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
      a. Recorded video is only available to UAPS;
      b. Requests to Facilities and Operations (F&O) from Faculties, Departments and Units will not be considered.
      c. Recorded video may be shared with Faculties, Departments and units at the discretion of UAPS as part of an investigation.

Refer to Appendix A: Security Services Guidelines and Matrix for further information on responsibilities and costs associated with the different types of security systems available.

DEFINITIONS

Any definitions listed in the following table apply to this document only with no implied or intended institution-wide use. [▲Top]	
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.
University owned and leased	University owned and leased rural lands are large rural land blocks

rural lands	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.

FORMS

There are no forms for this Procedure.. [▲Top]

RELATED LINKS

Should a link fail, please contact uappol@ualberta.ca. [▲Top]

Access Control/Security Systems Procedure Appendix A - Security Services Guidelines & Matrix (UAPPOL)

Lenel System (Lenel)

Lock Changes, Key Request and Key Control Procedure. (UAPPOL)

Operations and Maintenance (University of Alberta)

Control Centre Alarm Monitoring and Response Procedure (UAPPOL)

Information and Privacy Office (University of Alberta)