

Original Approval Date: June 27, 2005 Most Recent Approval Date: January 31, 2012

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 University procedure extends to all members of the University community.

Overview

The University of Alberta strives to provide a safe, comfortable, secure learning and working 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 installing an access control/security system
- identify the responsibilities for granting access
- identify who is responsible for costs associated with the installation, maintenance and monitoring of access control/security systems
- identify the process for requesting a security assessment
- identify centrally supported services vs. services paid for by user groups
- identify security solutions available to faculties, facilities and external consultants

PROCEDURE

INSTALLATION OF SYSTEMS

1. SECURITY SYSTEMS

All faculties, departments and units must consult with University of Alberta Protective Services if they are considering the installation of security systems within their assigned space. Protective Services will only be responsible for monitoring and responding to Protective Services approved security related alarms and as such must be involved in the selection, design and implementation of all security systems. This applies to intrusion alarm systems, video surveillance, blue phone alert systems 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. If deemed necessary a formal security assessment will be conducted under Protective Services' oversight.

2. ACCESS CONTROL SYSTEMS

Standard practice is to install keyed locks. If a convenience key card access controlled door is requested, this can be installed with or without alarm monitoring. This will be determined in conjunction with Protective Services and F&O and will fit one of the following two profiles:

- a. Convenience key card access doors which are not actively alarmed or monitored
- b. Convenience key card access controlled doors which are to be alarm monitored for intrusion. These doors must have a video surveillance camera nearby, which will facilitate monitoring that door from a remote location.

All access control implementations on all campuses shall be based upon a standard centralized system and will operate on the F&O FMNet network. Non-essential network traffic is not permitted.

Access Control Systems will be managed by the Access Control Administrator (ACA). The ACA will be responsible for the database associated with the access control system doors; for granting access privileges to central support units such as Protective Services, Environment, Health & Safety (EH&S), trades and building services; for providing detailed requirements for ACS design; and for interfacing with Faculty-based access control systems administrators (FACA).

Faculties, departments and units are responsible for learning how to use the access control system database (training provided through ACA), and for providing the administrative support (Faculty Access Control Administrator) for initial and ongoing management of the card access privilege database for their specific areas of responsibility within their building.

ACCESS CONTROL

1. EXTERIOR / PERIMETER DOOR ACCESS CONTROL

Building exteriors/perimeters are the responsibility of F&O to maintain and monitor. F&O is responsible for assigning access privileges to central support units such as Protective Services, EH&S, trades and building services. A Faculty Access Control Administrator (FACA) is responsible for assigning access privileges to the perimeter doors for their staff and students. The number of exterior doors to be accessible after hours will be limited.

2. INTERIOR DOOR ACCESS CONTROL

Interior doors are the responsibility of the faculty, department, or unit. F&O is responsible for assigning access privileges to central support units such as Protective Services, EH&S, trades and building services. A FACA is responsible for assigning access privileges to the interior doors for their staff and students. 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.

RESPONSIBILITIES AND COSTS

1. TECHNOLOGY RESPONSIBILITY

Currently Protective Services has technology responsibility for intrusion alarm systems and video surveillance systems. F&O has technology responsibility for Access Control Systems.

Protective Services must approve the design of all proposed intrusion alarm & video surveillance installations; F&O and Protective Services must approve the design of all proposed Access Control System implementations.

Protective Services and F&O will select security and access control system technologies and system manufacturers that are approved for installations on campus. All systems must conform to these selected technologies and manufacturers.

- a. All access control implementations on all campuses will be based upon a standard centralized system.
- b. All security systems including video surveillance cameras and intrusion alarms must be able to work within the standard centralized system thereby facilitating alarm routing to Protective Services.
- c. Further details are available from Protective Services and F&O.

2. ALLOCATION OF COST RESPONSIBILITIES

Responsibility for costs includes the cost of installation, maintenance/repair, and replacement, as well as additional costs that may be incurred including monitoring fees and per alarm response costs.

- a. Protective Services is responsible for security systems on the exterior grounds of the campuses, such as the blue phones, alert systems and video surveillance.
- b. F&O is responsible for the access control systems at building exterior/perimeter doors; with the exception of systems resulting from a major renovation or capital project. The cost of installation of new or modifications to existing exterior or perimeter security and/or access control systems resulting from a major renovation or capital project are to be borne by that project.
- c. All security and access control systems installed in the interior of buildings are the responsibility of the faculty, department or unit. This includes all costs for design, installation, implementation and connection to the existing infrastructure, including access card costs, as well as on-going system repair, maintenance and administration.
- d. Alarm response: more than 3 alarms in a 3 month period will result in a usage charge which will be consistent with external agency charges (consult with Protective Services for current charges).
- e. Annual maintenance allowance for internal doors: the Faculty is to carry the budget for this (amount to be determined).
- f. 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.

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 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 1 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)

Identity Policy (in development Provost & Vice-President (Academic))

[Lenel System](#) (Lenel)

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

[Operations and Maintenance](#) (University of Alberta)

[Security Services Matrix](#) (University of Alberta)