Access Control/Security Systems Procedure
Appendix A– Security Services Guidelines & Matrix

Office of Administrative Responsibility: Operations & Maintenance (Facilities & Operations)
Approver: Vice-President (Facilities & Operations)
Vice-President (Finance & Administration)

A security matrix was developed to provide a guideline of security services available to assist faculties, facilities 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. University of Alberta Protective Services provides assistance and reviews when questions or concerns arise.

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. These enhanced services come with a 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 administer and maintain records of key holders and authorize the issuance of additional keys. This affords maximum flexibility to the faculties, however minimizes the actual security protection offered. The maintenance of accurate records by the faculties 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 issuing of these keys is highly controlled and documented by the Facilities & Operations Lockshop. These two features improve 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 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/group which lost the key.
Convenience Card Access (On line-local alarm – no response):

This is an on-line card reader which 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 or facility administrator. Facilities 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.

Remote Monitoring Precision Response:

This level of security requires the installation of a card reader and a camera solution to assess a response situation prior to entry into a protected premise. The camera performs two functions; a live video feed to Protective Services is established when a security event initiates a response. The video feed is only activated during an emergency event and is automated to provide a pop up alarm in Protective Services. During specified periods the camera will act as a motion detector within the protected space. This motion detection feature provides an additional level of alarm detection to the defined space as it confirms an intrusion situation. The installation of a camera and the confirmed video verification of intrusion will prioritize an immediate alarm response from Protective Services. The annual fee for service shown in the matrix is based upon the security industry rates for this level of response services.

Local Intrusion Alarms:

This is best described as a commercial grade home intrusion burglar system. It utilizes phone lines or Ethernet for dialing and connecting to Protective Services to advise of an intrusion. It utilizes a keypad to arm and disarm an alarm detector in the protected space. It does provide for a mechanism that if a protected space is not armed for detection by a specific time that a message will be delivered to Protective Services. Protective Services will, during a routine patrol, check the premises to ensure the space is locked and advise the system owner by phone that the space is not armed. This is not a prioritized call that receives immediate response as no confirmation of intrusion has been received.

Open/Close System Reporting (Arming):

Opening and closing monitoring applies to premises that already have an intrusion (often called a burglary) system installed. The intrusion system notifies the control centre when the system is disarmed (open) and when it is armed (closed). The intrusion system is monitored within a given range of predefined hours. A software package will check whether the system is armed at the predetermined time. In the event the intrusion system has not been armed, a notification is generated to advise Protective Services the area is unprotected. Protective Services will then phone the area contact person who may come and arm the facility. Failure to open a premises at a requested time can also be monitored in a similar fashion.

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: (2012 estimated Canadian dollars)
   a. $5,000 per Access Control System (ACS) door with card access control (i.e. door with a card reader and electric lock)
   b. $4,500 per ACS door that is electrically controlled, but without a card reader
   c. $1,000 per door that is only roughed in for potential future ACS installation
   d. $2,000 per floor for an elevator requiring ACS
   e. $2,000 per video camera
   f. $2,500 per alarm system

   These are guidelines only. Actual costs will be dictated by features, site conditions, equipment locations, etc. Ensure that budget estimates are updated regularly during the design process. Contact Operations and Maintenance for current cost estimates.

2. Protective Services and Facilities & 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.

RELATED LINKS

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

Security Services Matrix (University of Alberta)