Scope

The scope of the keyless access upgrade project is to provide increased security and public safety by deploying electronic access controls, door status monitoring/security systems and rekeying the perimeter access points of all major University buildings. Effective physical and electronic security is essential in providing security, access and protection to University students, personnel and assets and to mitigate threats or hazards, either natural or human-made.

Depending on building design and layout, access points will operate in the following manner:

1. Designated perimeter doors will be electrically locked and unlocked according to electronic schedule, but capable of Cat Card Reader entry after hours or on weekends.
2. Secondary perimeter doors will be electrically locked and unlocked according to electronic schedule but without a Cat Card reader.
3. Egress only doors will remain locked at all times
4. All perimeter doors will be equipped with door status contacts and have dog down devices removed after rekeying.

After hours building access will be granted by presenting a valid UA Cat Card, creating an audit trail. Building entrance doors will be rekeyed off building masters reducing the liability of lost or stolen keys. Emergency override keys will only be issued to emergency responders. The locking and unlocking of designated entry doors will be accomplished electronically, according to established schedules.

Benefits

1. Provides building access for faculty, staff and students, without the need for metal keys.
2. Access to multiple buildings can easily be added or removed.
3. The extended liability of stolen or lost building entrance keys will be diminished.
4. An audit trail can be provided to effectively document activity at each door
5. Perimeter door lock and unlock schedules for buildings can be adjusted as needed.
6. UAPD can be notified if entry doors are forced open or propped open.
7. UAPD- Perimeter doors on a building or group of buildings can be remotely locked in the event of an emergency or threat situation.

In May 2011, The University of Arizona Administration building became the first University building to be upgraded to the new security protocol. The building's perimeter doors were converted to electronic access control and were then rekeyed with very limited key access to the building's perimeter doors. FM's goal is a five year plan to provide the same level of security and access to all major University academic buildings.

1. Department & Building Managers Responsibilities

a) Building managers, working in conjunction with the departments, are responsible to designate individuals to act as primary and secondary *Department Access Coordinator's* (DAC's). A minimum of 2 DAC's, but not more than 4, must be assigned per building, dependent on the number of departments housed in that building.

b) The building Manager may serve as the primary DAC if they choose, or they may delegate other individuals in the building to serve as primary or secondary DAC's. The DAC's will work with

Facilities Management and the *Third Party Security Vendor* in maintaining the department's access control and security systems program. Failure to designate a secondary DAC could delay the processing of access transactions when the primary DAC is unavailable.

c) Departments are responsible for controlling electronic Cat Card access to building perimeter doors and to all areas assigned to, or under the department's control and responsibility.

d) The department authorizing access for an individual is responsible for removing, returning or revoking that access as required. This includes any *metal keys* **(**see FM key issuance & return guidelines)**,** or *electronic access devices* issued to allow access to department controlled areas**.**

e) Keyless access installed on a building's interior doors: Departments are responsible for all costs related to interior door keyless access component repair or replacement, upon expiry of the two year warranty provided by the *Third Party Security Vendor*. Abuse or negligence is not covered under the two year warranty. This includes any interior door keyless access installations performed after the original construction of the building.

- *Exception: Interior doors utilizing Cat Card keyless access that were part of the original building construction project will be maintained by Facilities Management (excluding abuse or negligence).*

2. Department Access Coordinator (DAC) Responsibilities

a) The DAC will have overall responsibility for the management of electronic Cat Card access to building perimeter doors and other Cat Card access areas under the control of the department.

b) DAC's are responsible for granting or removing Cat Card authorization for user access to building entrances and other areas controlled by the department. This includes granting or removing access for new employees, departmentally sponsored visitors (DSV), retiring employees or terminated employees.

c) DAC's are responsible to routinely contact the *Third Party Security Vendor* to re-authorize individual Cat Card users, based on the level of access and security required. The DAC should only authorize the minimal amount of access required for an individual to perform their assigned duties.

d) The DAC's will confirm that any means of electronic access to building perimeters or other University areas, under their control, has been terminated at the time the user or employee leaves the department or the University.

e) The DAC's will maintain accurate records for individuals that have been granted electronic access to building perimeter doors and all other areas under control of the department.

f) *Third Party Security Vendor* will send an annual report to the DAC of all active electronic access users, authorized by the department, with access to areas under the department's control. The DAC can also choose to implement and manage automatic expiration of user access if they determine this level of management is required. There may be security and risk levels that warrant audit reports being provided more frequently. Accommodations will be made to comply with those requirements. Each of the active users will need to be re-authorized by the DAC, for the users to have continued access to the areas under control of the department. This report will list, at minimum, the person the department has authorized access to; the areas under control of the department and level of access granted. The department will review this listing to confirm the individuals listed are still active with the department and the access is appropriate for each person’s position. It is the responsibility of the DAC to send this updated access information to the *Third Party Security Vendor*.

g) The DAC’s will alert Facilities Management and the *Third Party Security Vendor*, immediately, of any changes involving the DAC.

3. User Responsibilities

a) The user, which could be a student, faculty, staff, visitor, contractor, subcontractor, or any other individual affiliated with the University of Arizona, is responsible for securing and safeguarding any *access device* they have been issued. This includes but is not limited to, metal keys, *Cat Card*, Access Card, proximity *device*, biometric *device*, combination, PIN code, or any device used to gain access to any University buildings or areas under the control of, or maintained by, the University of Arizona.

b) Users are individually responsible to proactively confirm their Cat Card and pin code work properly, prior to the necessity of afterhours building access, weekend access or to attend to any type of critical research in University buildings. Failure to do this could result in delays in gaining building access.

c) If any *access device*, for which the user is responsible is lost, stolen or compromised the user must report it immediately to the building DAC and the building manager, or for contractors- their University point of contact and the FM Keydesk. In addition to the reporting procedure listed above, if metal keys are lost or stolen the user, department or company must contact the FM key desk and follow key desk procedures regarding lost or stolen keys.

d) Upon leaving the department or termination of employment with the University of Arizona, either voluntarily or involuntarily, individuals are required to return all issued *access devices* to the issuing department, with the exception of metal building keys which must be returned to the Facilities Management Keydesk so the key return can be properly documented.

4. Facilities Management Responsibilities

Since each University building is unique in design and purpose, Facilities Management will coordinate with UAPD, the departments, and the *Third Party Security Vendor* to develop and implement a workable plan to secure and schedule buildings converted to the new security protocol.

The Facilities Management Locksmith Shop is the only facility authorized to originate or duplicate metal keys to any building or other area owned, operated or controlled by the University of Arizona. Individuals in possession of an unauthorized University building key may be referred to UAPD subject to *ARS §13-3715*.

a) Facilities Management will oversee all processes involving University of Arizona access control systems and security systems. The Facilities Management Locksmith Shop will serve as the central point of contact for physical, electro-mechanical and electronic access control systems.

b) All electronic and mechanical access control installations, repairs or modifications must comply with the following to ensure coordination, review, code compliance, security and safety.

- Access control device installations must meet all applicable Federal, State and Local laws and code requirements; be installed in accordance with manufacturer’s specifications and the current University of Arizona Manual of Design Specification Standards.

c) Departmental staff, students, vendors or volunteers may not perform work on University doors, mechanical locks or access control systems, without prior written approval from the Assistant Vice President, Facilities Management or their appointed designee. The Assistant Vice President or their appointed designee may at any time rescind this written approval.

d) Facilities Management will oversee and coordinate mechanical, electro-mechanical and electronic access control and security system installations, repairs, upgrades, service, programming, planning, and review.

e) Facilities Management will be responsible for Facilities Management employees’ access to University buildings and property, while performing their duties as part of Facilities Management responsibilities to the University of Arizona.

f) Facilities Management will coordinate access for University of Arizona campus support units to include, but not limited to, UAPD, Fire Safety, UITS, Office of Radiation, Chemical, and Biological Safety, Risk Management, Real Estate Administration and PD&C, in the performance of their duties in support of the University of Arizona. This does not release each of the above units of their respective departments responsibilities stated in (1a – 1e and 2a-2g).

g) Facilities Management will correct any projects, conducted without prior approval of Facilities Management and in violation of this policy, with all costs being charged to the responsible department.

h) Facilities Management is responsible for all costs related to keyless access component repair or replacement on general or public building entrances not directly related to a department.

- *Exceptions: Buildings that are classified as auxiliary units*

i) Facilities Management is responsible for all costs related to keyless access component repair or replacement on interior doors, utilizing Cat Card keyless access, that were part of an original building construction project.

- *Exception: Card readers on Buildings that are classified as auxiliary units*
- *Exception: Card readers on interior doors that are damaged due to abuse or negligence i.e. departmental staff knocking off a reader by striking it with a push cart*

5. Keyless Access After Hours Support Procedure

The following procedure provides direction to building end users that require support with the Keyless Access system after hours.

The following steps will be used in the event that a user, expecting to have access to a building, experiences trouble with the keyless access system:

a) Building user should contact Amer-X at 626-9346 and provide the Amer-X operator with the following information. Operator will let the user know a technician will call them back within 15 minutes or less.

   1) First name
   2) Last name
   3) 16 Digit Cat Card number
   4) Building name, door description or room number
   5) Description of problem
   6) Call back number

Amer-X Operator will contact Amer-X on call technician. On call technician will confirm in the DSX system that the user is in the system with the correct Cat Card and Access Level.

The on call technician will check history in DSX to confirm if user is being granted access, denied access by level, or denied access by time zone. On call technician will call user back to help resolve the issue the user is having.

a) If user is in the system with the correct information and access, but the door is not working because of equipment failure, Amer-X technician will respond out to the site within 30 minutes to resolve the problem with the equipment. The Amer-X technician will contact the FM GMM or the on-call FM locksmith to meet them at the building. The user will be given access to the door once the Amer-X technician arrives on site to meet the GMM or the on-call locksmith.

b) If the user is in the system but is denied access because they don't know their PIN number, they don’t remember their PIN number or the PIN number the user provides to Amer-x does not match the PIN number registered in the access control system, they will be asked to contact their building DAC to get their correct PIN or update their PIN.

c) If the user is in the system with the correct information but are denied access because they are outside their days or times of access they will be asked to contact their DAC.

d) If the user is in the system with the correct information but the user does not have their Cat Card with them to swipe at the door they will be denied access by the Amer-X technician.

In the event that the users Cat Card was left in the building, the Amer-X technician will recommend the user contact UAPD at 621-8273.UAPD will determine whether they have resources available to send an officer to the building, to escort the user to their Cat Card. Alternatively, the user may contact the building DAC or another building user to assist them with gaining access to the building. Due to security concerns and for auditing purposes, Amer-X will not remotely unlock a keyless access door for a user, even if proper information is provided, since the identity of the caller cannot be established via telephone.