Policy Contents

- Purpose and Summary
- Scope
- Definitions
- Policy
- Compliance and Responsibilities
- Related Information*

Policy Information

Responsible Unit:
Facilities Management
Phone:
(520) 621-3000
Email:
FM-Keydesk@email.arizona.edu [1]

Purpose and Summary

Physical and electronic security is essential in providing security, access, and protection to University of Arizona students, personnel, equipment, buildings, and resources. Universities are popular targets of theft from both internal and external threats. Access to University buildings is a privilege, not a right, and implies user responsibilities and accountability.

The purpose of this policy is to regulate access to University of Arizona property and ensure that any individual, college, department, operating *unit,* or program within the scope of this policy is aware of their respective responsibilities when assigned Cat Cards and building keys. This policy will help provide a safe and secure campus environment through the diligent control of electronic access devices and building keys.

Italicized terms used in this policy are defined in the Access Guideline Terms.

Scope

This policy and all implemented standards and procedures will apply to all individuals using any *device* to access University buildings and or resources, including but not limited to:

- Vice Presidents, Deans, Directors, and Department Heads
- Affiliates, associates, and volunteers

- Faculty, appointed personnel, staff, and students
- Third-party vendors, contractors and their agents

Definitions

Access Guideline Terms

“Access Device/s”: See definition of “Key.”

“CatCard”: University of Arizona ID (CatCard) can be used as a “Key.” See definition for Key.

“Department Access Coordinator (DAC)”: Person designated by a Vice President, Dean, Director, Department Head, or Building Manager to be responsible for authorizing and processing all access control transactions for the department

“Device”: See definition of “Key.”

“Electronic Access Security”: Any electronic or electro-mechanical locking device, using a key, that can be controlled from a site that is remote from the device. Any device that can be programmed or reprogrammed, that could have users added, modified, or removed from a site that is remote from the device. Any device that can be opened, unlocked, locked, or disabled from a remote location.

“Key”: Any means or device used to lock, unlock, open, or gain access into a secured area. This includes but is not limited to metal key, combination, keypad code, keypad PIN code, CatCard, Access Card, magnetic, proximity, biometric, RFID (radio frequency identification), or any combination of devices used to lock, unlock, open, or gain access to a secured area.

“Mechanical Security”: Mechanical locking device requiring no electrical power to open, lock, unlock, or secure access to an area. Mechanical locking devices use a metal key or other apparatus.

“**Monitoring Center**”: Underwriters Laboratories (UL) listed monitoring center that provides 24-hour, 7-day-per-week off-site monitoring of security, fire, and other alarms and dispatches security, police, and/or fire personnel when an alarm is received. Monitoring center can be a third-party vendor.

“Physical Security” Composed of Mechanical Security, Electronic Access Security, and a Security System.

Security Levels

Level 1 - "Basic Security": These areas are typically unlocked during business hours, allowing access by University personnel or the general public. After hours these areas are secured and access is by University CatCard and use of PIN. University support units will have access to these areas. Security Systems are also integrated into this program and may be required to be armed and disarmed by authorized personnel, as necessary, to maintain the desired level of security.

Level 2 - "Enhanced Security": Areas that are mechanically and electronically locked at all times, including during normal business hours, require University access card to gain entry each time, and may also require use of PIN. University support units will have access to these areas. Security Systems are also integrated into this program and may be required to be armed and disarmed by authorized personnel, as necessary, to maintain the desire level of security.

Level 3 - "High-Risk Security": Areas that by federal, state, or local laws or code have restricted access, or are restricted by University policies and/or procedures. These areas may require higher security access control devices such as biometric control devices. In some cases access by University support services may be restricted or limited and may require that support services be escorted by approved department personnel. Security Systems are also integrated into this program and may be required to be armed and disarmed by authorized personnel, as necessary, to maintain the desire level of security.

“Security System”: Devices to detect unauthorized intrusion or breach of a security parameter and notify a local or remote Monitoring Center.

"Third-Party Security Vendor": Pursuant to the “Policy for CatCard Keyless Access Security and Security Systems for New Construction, Alterations, and Renovations of Existing University Buildings” a third-party sole-source vendor has been selected and is reviewed on an annual basis to ensure the level of service meets University of Arizona standards. This vendor provides a 24/7 support staff, in conjunction with a UL-listed monitoring center, to monitor all of the designated security systems.

"Unit": Any University college, department, program, or other operating unit.

Policy

An essential element of security is maintaining adequate access control so that University facilities may only be accessed by those that are authorized. Issuance of access devices should be careful, systematic, and audited, as inadequately controlled access devices result in poor security. Each department will adopt and implement this policy and follow the Facilities Management guidelines relating to electronic access and the issuance of metal keys for building access. All units and departments within the scope of this policy are responsible for compliance to ensure the protection of University resources.

Non-Compliance

Failure by individuals, departments, or units to follow this policy and procedures may be subject to disciplinary action in accordance with Arizona Board of Regents and University of Arizona policies and procedures as appropriate. Violations of this policy may result in additional costs to the individual, department, or unit.

Exceptions

The Assistant Vice President of Facilities Management or his/her designee may grant exceptions to this policy or related procedures after a security risk assessment. The Assistant Vice President may at any time rescind any exceptions to this policy or procedures based on a new risk assessment or abuse of any exceptions granted. Residence Life will be an exception to this policy as that unit has its own keyless access policy due to the unique living arrangements.

Compliance and Responsibilities

Facilities Management is responsible for establishing electronic access and metal key policies and supporting procedures. Pursuant to the Senior Vice President for Business Affairs “Policy for CatCard Keyless Access Security and Security Systems for New Construction, Alterations and Renovations of Existing University Buildings,” effective July 1, 2000. Facilities Management

regulates metal key issuance and electronic access systems and maintains mechanical and electronic locking devices and all related door hardware specification, design, deployment, maintenance, and integration with other *security systems*.

Responsibility for access to University buildings and resources and for implementation of this policy rests with the **Vice Presidents, Deans, Directors,** and **Department Heads.** This overall responsibility may not be delegated. Specific responsibilities within this policy may be delegated within their respective units.

The **Assistant Vice President of Facilities Management** will have responsibility for

- Oversight of *Mechanical security*, *electronic access security*, alarm security, and the *Third-Party Security Vendor*.
- Development, revision, and oversight of this policy and related procedures.
- Enforcement of this policy.

The **Assistant Vice President of Facilities Management,** or his/her designee, will issue procedures and guidance to assist units in implementing this policy. This policy is the governing foundation for future policies and procedures related to *physical security* of campus buildings, property and resources.

Vice Presidents, Deans, Directors, Department Heads and **Building Managers** will work together to designate a *Department Access Coordinator* to serve as the primary contact between their respective units, Facilities Management and the *Third-Party Security Vendor* regarding matters relating to *physical security*. Facilities Management must be contacted immediately of any changes involving the *Department Access Coordinator*.

Related Information*

Electronic Access Guidelines [2]

FM Key Issuance & Return Guidelines [3]

Links
[1] mailto:FM-Keydesk@email.arizona.edu
[2] http://policy.arizona.edu/sites/default/files/uploads/ACCESS_GUIDELINES.pdf
[3] http://www.fm.arizona.edu/documents/LocksandKeys/UA%20Key%20Issuance%20and%20Return%20Guidelines.pdf