Published on *Policies and Procedures* (https://policy.arizona.edu)

Home > Facilities Electronic Access/Key Control Policy

Policy Contents

Policy Information

Effective Date:
December 16, 2021
Last Revised Date:
December, 2021
Responsible Unit:
Facilities Management
Email:
FM-Lockshop@arizona.edu [1]

Purpose and Summary

Physical and electronic security is essential in providing security, access and protection to University of Arizona (University) 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 property and to ensure that any individual, college, department, operating unit or program, within the scope of this Policy, is aware of their respective responsibilities when assigned CatCards 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.

Scope

This Policy and all implemented standards and guidelines 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;

- Faculty, staff, and students (Undergraduate, Graduate and Professional);
- Third party vendors, contractors, designated campus colleagues (DCC’s) and their agents.

Definitions

Access Device/s: See definition of Key.

CatCard: The official University of Arizona identification card.

Department Access Coordinator (DAC): Person designated by the Vice Presidents, Deans, Directors, Department Heads and Building Managers to be responsible for authorizing and processing all access control transactions for the department.

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, 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 Access Device used to lock, unlock, open or used to 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: Locking device requiring no electrical power to open, lock, unlock, or secure access to an area, which 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 security vendor.

Physical Security: Comprises Mechanical Security, Electronic Access Security and a Security System.

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

Security Levels:

Level 1 – Basic Security: Areas that 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. An additional key pad may also be integrated into the Security System, requiring it 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 and requiring University CatCard to gain entry each time and may also require use of PIN. University support Units will have access to these areas. An additional key pad may also be integrated into the Security System, requiring it to be armed and disarmed by authorized personnel, as necessary, to maintain the desired level of security.

Level 3 - High Risk Security: Areas that by Federal, State, or local laws or code restrict access, or are restricted by University policy. 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 support services be escorted by approved Unit personnel. An additional key pad may also be integrated into the Security System, requiring it to be armed and disarmed by authorized personnel, as necessary, to maintain the desired level of security.

Third-Party Security Vendor: A security vendor that provides a 24/7 support staff, in conjunction with a Monitoring Center, to monitor all the designated Security Systems.

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

Policy

Only authorized individuals may access University facilities.

Each Unit and all individuals subject to the Scope of this Policy must follow the Electronic Access Guidelines and Facilities Management Key Issuance and Return Guidelines relating to electronic access and the issuance of metal keys for building access. All Units within the scope of this Policy are responsible for compliance to ensure the protection of University resources.

For University facilities, 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 approving access to University buildings and resources and for implementation of this Policy rests with the Vice Presidents, Deans, Directors, and Department Heads. Responsibility for approving access may not be delegated. Specific other responsibilities within this Policy may be delegated within the 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 guidelines.
- Enforcement of this Policy as described in this Section.

The Assistant Vice President of Facilities Management, or their designee, will issue guidelines to assist Unit compliance with this Policy. This Policy is the governing foundation for future policies and guidelines 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 DAC 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 notified immediately of any changes involving the DAC.

The Assistant Vice President of Facilities Management or their designee may grant exceptions to this Policy or related guidelines after a security risk assessment. The Assistant Vice President may at any time rescind any exceptions to this Policy or guidelines based on a new risk assessment or abuse of any exceptions granted.

Compliance and Responsibilities

The Assistant Vice President of Facilities Management is responsible for the oversight of and compliance with this Policy.

All Units within the scope of this Policy are responsible for compliance to ensure the protection of University resources.

Failure by individuals or Units to follow this Policy and associated guidelines may result in disciplinary action in accordance with Arizona Board of Regents and University of Arizona policies. Violations of this Policy may result in an individual losing access to a facility, a restriction on receiving additional keys, and/or additional cost to the individual or Unit, including paying for the facility or area to be rekeyed.

Related Information*

Electronic Access Guidelines [2]

Facilities Management Key Issuance & Return Guidelines [3]

Due to its unique scope of responsibilities on campus, Housing & Residential Life maintains an independent electronic access policy, metal key policy, and supporting procedures under the authority of the Senior Vice President for Student Affairs and Enrollment Management. Housing & Residential Life will coordinate and implement access safety plans with Facilities Management and University of Arizona Police Department (UAPD) to ensure the interoperability of the CatCard system.

Revision History*

07/28/2022: Updated responsible unit email address.

12/16/2021: This Policy replaces Access to University Building Restricted Areas (BUS-100).

Source URL:https://policy.arizona.edu/facilities-and-safety/facilities-electronic-access-key-control-policy-0

Links
[1] mailto: FM-Lockshop@arizona.edu [2] https://www.fm.arizona.edu/documents/LocksandKeys/AG-101%20%20ELECTRONIC%20ACCESS%20GUIDELINES.pdf [3] https://www.fm.arizona.edu/documents/LocksandKeys/UA%20Key%20Issuance%20and%20Return%20Guidelines.pdf