Williamson County
Facilities Management

Physical Access Control Policy

Sensitivity: Controlled
Criticality: Critical
Primary Type: Policy and Procedure

Summary

Purpose

Williamson County ("County") is committed to providing a safe and healthful workplace for all County employees and those who require access to County facilities. As part of this goal, this Policy is instituted for the purpose of promoting a secure facility environment and for maintaining a comprehensive system to efficiently manage the dissemination of Access Control Assets throughout County facilities.

Scope

This Policy shall apply to all individuals seeking access to County facilities and Secured Work Areas, including but not limited to, all Public Officials, County employees, volunteers, interns, and non-County individuals/entities. Departments may adopt more detailed policies and procedures in addition to this policy.

Definitions

Access Administrator
A person designated by a Public Official or Department Head to request and manage Access Control Assets and access levels to a particular County office or facility.

Access Control Asset
The tangible or intangible means to authorize entry into buildings and Secured Work Areas, including but not limited to access codes, keys, fobs and badges.

Access Control Asset Holders
Individuals who are approved to possess Access Control Assets, including Public Officials, County employees, volunteers, interns, and non-County individuals/entities (e.g., vendors, contractors, property lessees, guests, etc.).

Access Control Procedures
Williamson County Physical Access Control Procedures, as amended, established by the Facilities Management Department.

Access Control System
Equipment with audit capabilities to track and monitor badge usage.

Department Head
The highest-ranking County employee in a department created and supervised by the Commissioners Court.

Policy
Williamson County Facility Physical Access Control Policy.

Public Officials
Elected and appointed officials who are provided workspace in County facilities.

Secured Entry
Any door or access point to a County facility that requires an Access Control Asset to gain entry.

Secured Work Area
A County facility or an area within a County facility in which access is controlled and the general public are normally not permitted to enter.

Roles and Responsibilities

- All individuals seeking or already granted access to County facilities are required to adhere to this policy and associated procedures.
- Public Officials and Department Heads should inform their employees, volunteers, and interns of this content and ensure each employee fully understands and undertakes to comply with this content.

Policy

No individual shall access a secured entry or Secured Work Area of a County facility without authorization pursuant to this Policy and corresponding procedures. The Williamson County Facilities Management Department shall implement this Policy and shall maintain an Access Control System that manages badge access to County facilities.

A. Access Administrator Delegation and Responsibilities

1. Each Public Official, Department Head, or non-County individual/entity shall designate a person who will act as a liaison between the Facilities Management Department and the office or facility. This designated person will serve as Access Administrator and will manage Access Control Assets as determined by this Policy and the Access Control Procedures. (May include more than one designated individual, best practice to have a primary and backup for continuity.)

2. Requests for new, replacement, or deactivation of an Access Control Asset as well as requests to change or remove access levels must be made by the Access Administrator. Additional approval by the Public Official, Department Head, or non-County individual/entity may be required for some Secured Work Areas.

3. If the Access Administrator receives a facility key or any other Access Control Asset from an Access Control Asset Holder, the Access Administrator shall immediately return the key or Access Control Asset to the Facilities Management Department in person or in designated dropboxes.
4. If the Access Administrator determines that an access code is no longer needed and/or needs to be changed, the Access Administrator shall immediately notify the Facilities Management Department. The Access Administrator shall also notify the Facilities Management Department on or before an Access Control Asset Holder's last day of service.
5. An Access Administrator shall not retain any Access Control Asset in anticipation of an employee replacement, transfer, or termination.
6. It is the responsibility of the Access Administrator to verify that all Access Control Assets are accounted for, and, prior to the beginning of each new fiscal year, the Access Administrator shall review a list of Access Control Assets issued to each Access Control Asset Holder to ensure that such records remain accurate. In the event such records are not accurate, the Access Administrator shall notify the Facilities Management Department of such inaccuracies.
7. An Access Administrator will be the point of contact and assist the Facilities Management Department ensuring compliance with any audit of Access Control Assets.
8. The Access Administrator shall follow the Access Control Procedures.

B. Access Control Assets

1. General

a. All Access Control Asset Holders may be required to clear a background check prior to the issuance of an Access Control Asset.

b. Access Control Asset Holders shall keep Access Control Assets secured at all times. Access Control Assets shall not be left unsecured or unattended, such as in vehicles or in unlocked desk drawers.

c. While entering and exiting a County facility using an Access Control Asset, each Access Control Asset Holder shall ensure that all secured doors close behind them. Secured entries and Secured Work Area doors should never be propped open.

d. It is a violation of this Policy to allow unauthorized persons to enter a secured entry or Secured Work Area or allow other individuals or employees to gain access to a secured entry or Secured Work Area without using their own Access Control Asset (also known as piggybacking or tailgating).

e. It is a violation of this Policy for an unauthorized person to enter or attempt to enter a secured entry or Secured Work Area.

f. Access Control Asset Holders shall not "loan" or transfer an Access Control Asset to another employee, non-employee, volunteer or other individual. Secured/Detention Facilities key exception: Section B.3.e

g. Access Control Assets may only be used to gain access to the areas and facilities necessary for the performance of the Access Control Asset Holder's normal/routine duties and responsibilities.

h. If an Access Control Asset is lost or stolen, the Access Control Asset Holder shall immediately report the lost or stolen asset to both the Facilities Management Department and the Access Administrator. An Access Control Asset Holder shall make reasonable efforts to locate a lost Access Control Asset.

i. Access Control Asset Holders shall return all Access Control Assets to the Access Administrator and/or Facilities Management Department upon separation from employment, retirement, resignation, transfer to another Public Official's office or County Department, project completion, completion of volunteer service and/or at the request of the Access Administrator.

j. With the exception of access to areas containing sensitive chain of custody items (e.g., ballots, evidence, etc.), authorized Williamson County Technology Services and Facilities Management personnel shall have the authority to access all County facilities and Secured Work Areas, including immediate access in case of emergencies or critical incidents.

k. All Access Control Asset Holders shall follow the Access Control Procedures.

2. County Badges

a. A County badge shall be issued to all County employees, officials, and other authorized individuals performing work at County facilities, i.e., Access Control Asset Holders.

b. A County badge shall be worn at all times while in a County facility. The County badge must be visible and not obstructed.

c. Badge holders who misplace or have forgotten their badge will not have access to Secured Work Areas. Temporary badges will not be issued to an individual by the Facilities Management Department.

d. Access Control Asset Holders are prohibited from possessing multiple County badges. All old, broken, or duplicate County badges shall be brought to the Facilities Management Department and/or the Access Administrator so that it can be appropriately destroyed or deactivated.

e. All Access Control Asset Holders shall return all badges/fobs to the Access Administrator, or designee in their absence, on the last day of County service or upon changing County departments or offices.

f. Key fobs will only be issued to current Elected Officials and Law Enforcement Officers employed by the County. A photo only badge will be issued for those electing a fob.

3. Facility Keys

a. It is a violation of this Policy to manufacture, cut, or duplicate any facility key by a person other than the County locksmith. Offenders will be subject to disciplinary action by the Public Official or County Department and denial of future Access Control Assets by the Facilities Management Department.

b. If an Access Control Asset Holder suspects that a facility key has been manufactured, cut, or duplicated, the Access Control Asset Holder shall immediately report such matters to the Facilities Management Department and to the Access Administrator. Access Administrators shall report such matters to the Facilities Management Department.

c. All Access Control Asset Holders shall return all facility keys to the Access Administrator in the event of an administrative leave of absence.

d. All Access Control Asset Holders should return all facility keys to the Access Administrator in the event of a planned leave of absence of more than two weeks in which the employee may not return.

e. Access Control Asset Holders are prohibited from possessing multiple keys of the same keyway.

f. Detention and Secured Juvenile Facilities keys shall not be removed from the detention facility. Keys must remain on the secured ring and be issued to appropriate personnel along with a method of tracking and stored in a secured lockbox between shifts and accounted for by the department daily.

4. Access Codes (Including Security Alarm Codes)

a. It is a violation of this policy for an Access Control Asset Holder to share an access code with any unauthorized individual.

b. If an access code has been shared with an unauthorized individual or is otherwise obtained by an unauthorized individual, the Access Control Asset Holder shall immediately report such matters to the Facilities Management Department and the Access Administrator. Access Administrators shall report such matters to the Facilities Management Department.

C. Charges for Replacement of Access Control Assets

The Access Control Asset Holder who loses or makes inoperable an Access Control Asset will be responsible for replacement costs of Access Control Assets. Access Control Asset replacement charges are as follows:

Grand Master Key	$200
Building Master Key	$150
Area/Suite Master Key	$100

DC Key	$50
Badge/ FOB	$20

Note: Lost key charges will be refunded if keys are found and turned into the Facilities Management Department within 30 days of loss.

If the lock-core of a lock must be changed for security reasons due to an Access Control Asset Holder losing a key to such lock, actual cost of re-keying will be determined by the Facilities Management Department and the cost may be charged to the County Department or Public Official's office who originally authorized said keys to the Access Control Asset Holder.

Corresponding Procedures

The Williamson County Facilities Management Department shall establish and administer Access Control Procedures consistent with this Policy, which describe the process by which control, dissemination, use, and possession of Access Control Assets to County facilities will be managed. These Procedures shall be accessible on the County's website and shall be reviewed and revised periodically by the Facilities Management Department to reflect changes in technology and best practices. Reviews must be conducted biannually and any revisions to the Procedures shall become effective thirty (30) days after posting to the County website. All Access Control Asset Holders shall be responsible for adhering to these Procedures.

Exceptions

Exceptions to facilities policies, standards, and procedures must be documented and approved by the Senior Director of the Facilities Management Department.

Violations

Violations of this Policy can lead to loss of access privileges by the Facilities Management Department, as well as possible disciplinary action by the violator's Public Official or Department Head up to, and including, termination. Violations of this Policy may also subject the violator to administrative/criminal investigation and prosecution.

Related Statutes, Policies, and Authorities

Contact Office

Except as otherwise stated herein, Access Control Asset Holders should contact their management with questions or for clarifications regarding this policy and any corresponding procedures. Public Officials and Department Heads should contact the Facilities Management Department with questions or for clarifications regarding this policy and any corresponding procedures.

Administrative Notes

Policy Class:	Physical Security
Policy Family:	Physical Access Control
Policy:	Physical Access Control
Standard:	
Control Reference(s):	
Responsible:	Facilities Management
Accountable:	Facilities Management
Consulted:	HR, County Manager, Legal, Audit, Sheriff's Office, Juvenile Services, Emergency Services, ITS
Informed:	

Revision History

Version	Date	Description
1.0	2/25/2025	Initial adoption