Standard Operating Procedure

Campus Wide Facility Access Control

Table of Contents

1.0 - INTRODUCTION

1.1 - General

The University of Texas at El Paso is committed to ensuring a safe and secure campus. This Standard Operating Procedure (SOP) describes the procedure and responsibilities for all parties involved in the requesting and granting keyed or electronic access to facilities.

1.2 - Objectives

The purpose of this policy is to provide adequate physical building security for persons and property through the use of access control devices and the control of keys issued, to assure appropriate access to work areas by employees in buildings on the UTEP campus, and to allow unrestricted access by University Police, maintenance and safety personnel to all campus areas for reasons of security, safety, and health.

1.3 – Overview

Facilities are responsible for the management of the University keying and electronic access control systems. That responsibility includes controlling the production, storage, and issuance of keys; the replacement or rekeying of lock cylinders; the acquisition of new keying systems; the maintenance of accurate records; and the cataloging of and adherence to key system authorizations. All locks and keys must be approved by Facilities Management before installation. Facilities Management is also responsible for the purchase, installation, and maintenance of campus-wide electronic access control systems. The Facilities Key Shop is responsible for stand-alone access locks.

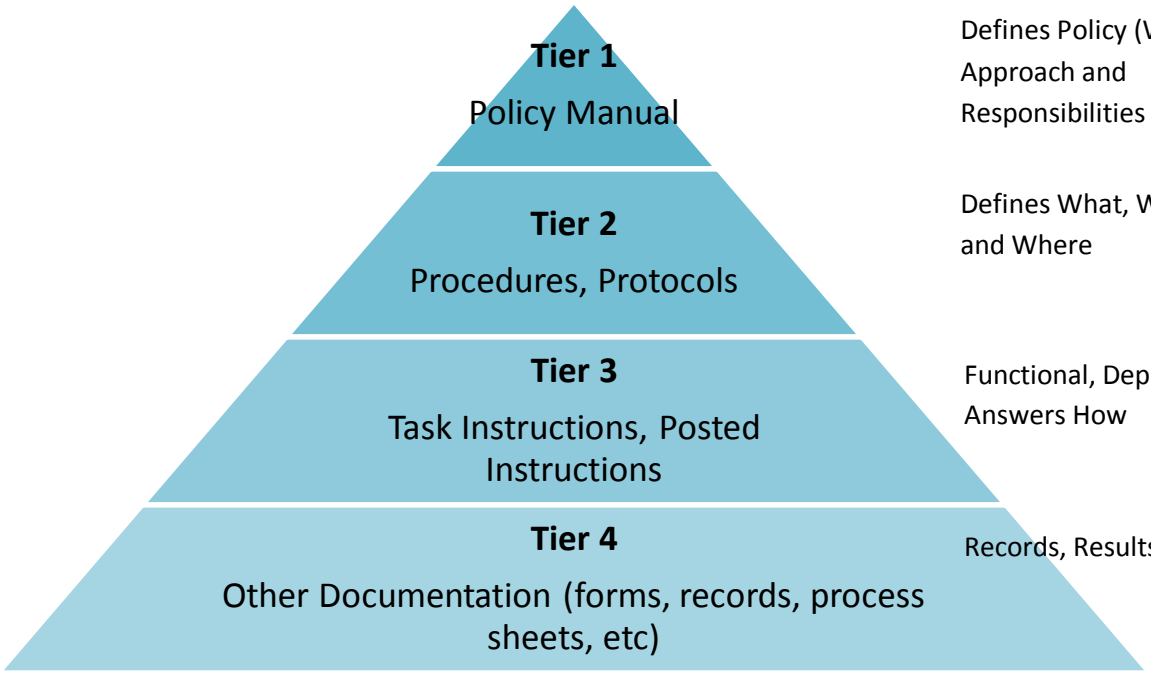
The UTEP Campus Police Department is responsible for overall campus security. Any deviation from established security policies and practices must be submitted to the UTEP Campus Police Department in writing for approval.

1.4 – Definitions

Term	Definition
Access Control	Control of entry/exit to an area by any means (mechanical or electronic means) *Mechanical Key System* - Any mechanical device used to operate a mechanically controlled mechanism for entry/exit to a controlled area. *Lockbox Systems* - An access control system designed for building access, used by service departments or police/fire personnel. *Card Access Control Systems* - A computerized access control system. An electronic or electro-mechanical device replaces or supplements mechanical key access and the Miner ID Card is used to unlock doors. The system provides entry access to various doors and enables automatic

	locking and unlocking of specific doors or groups of doors at prearranged times during the day.
Access Control Director	The Vice President for Business Affairs has been designated as the overall authority and delegated the responsibility for administration of this policy, procedures, approvals and issuance of all University access and is accountable for access and security of all campus facilities and property.
Access Control Administrator	The Associate Vice President Business Affairs, Facilities Management has been designated as the overall authority to implement this policy and procedures.
Access Control File	Critical records maintained by the Facilities Management - Access Control Shop, such items as key codes, key copy numbers, and Access Control database as well as departmental control access data.
Miner Gold Card	This is a multi-use identification card given to every student, faculty, staff and may be issued to authorized visitors. This card is distributed by the Miner Gold Card Office.
Access Control Supervisor	Designated individual within the Facilities Management - Access Control Shop who manages the keying system and access service delivery.
Space Steward	Person in a department responsible for appointing a Department Access Coordinator and Authorizing individual key requests within their specific department. This is reserved to Executive offices, Deans, Directors, Chairperson.
Trainer	Person responsible for training Key Holder of aspects related to certain building access requests. Trainers include EH&S Lab Safety Trainers, Level II protocol trainers, etc. The requirements for training are outlined in each Task Instruction related to Level II access requests.
Department Access Coordinator	Person delegated by the Space Steward to coordinate access requests, adherence and implementation of this policy.
Key Holder	Any University employee, student, volunteer, alumnus, or authorized visitor/vendor in possession of an access device (key/card)

2.0 - DOCUMENT SYSTEM



2.1 -Process:

2.1.1 - Tier I Documentation (Policies)

The purpose at this level of documentation is to state, in a concise and brief format, the overall policies, beliefs, and objectives of management on the operation and maintenance of the Facilities Access Control System.

These are traditionally internally driven documents that are written to conform and parallel other departmental or functional policies and procedures.

2.1.2 - Tier 2 Documentation (Facility Operations and Maintenance Procedures)

The second level of documentation is more detailed and addresses the procedure(s) for an activity or process, and identifies who is involved, what happens, and the critical control points. These procedures are organized on a functional basis.

2.1.3 - Tier 3 Documentation (Task Instructions)

This level of documentation is very detailed on "how": to accomplish one specific job, task or assignment. These may be references to existing documents, checklists or forms, or incorporated within a computerized maintenance management system. This entails work/job instructions which may stand alone or are part of a larger manual or policy.

2.1.4 - Tier 4 Documentation (Records)

The last level of documentation can include forms, records, reports and other documents used to summarize the results of the processes and provide evidence of conformance to requirements, goals and objectives.

3.0 – TIER 1 POLICY MANUAL

3.1 Policy Introduction

This standard operating procedure (SOP) describes procedures to request, grant, track and remove lab access to help ensure the security of our staff, faculty, students and facilities. This SOP shall be followed by all staff, students, faculty, contractors and visitors to the campus.

3.2 UTEP Security Access Levels

UTEP has two (2) access security levels.

3.2.1 Level I Description:

This is the basic access level that all students, staff and faculty have based on their enrollment or employment status.

3.2.3 Level II Description:

This is the highest access level associated to specific restricted spaces. Security approval at this level for a restricted space does not constitute automatic access to any other building doors within or throughout the campus.

Each of these spaces shall have its own access request, a detailed access request procedure listing proper training, protocol and a Space Steward's Contact information. This access request requires the designated Space Steward's approval requesting facility access for the Key Holder. Those who do not follow the access protocol for these spaces will face immediate disciplinary action up to and including dismissal and prosecution.

3.3 Granting Access

Access to buildings, offices, and other facilities may be granted to all staff, students, faculty, contractors and visitors to the campus upon proper authorization by respective Space Steward.

3.4 Responsibilities

3.4.1 Access Control Director - Vice President for Business Affairs

Designated as the overall Access Control Director and is responsible for or may delegate the following items:

1. Approves all new access control systems and modifications to existing systems.
2. Ensures appropriate authorization of all key fabrication and electronic access requests.
3. Directs Access Control Manager to conduct a key control record audit as needed.
4. Ensures the involvement of Facilities Management and Campus Police in the design and planning of new and modified access control systems.
5. Requests designated Internal Security Auditors, Access Control Shop and/or Campus Police employees to conduct reviews of campus departments and units to determine the adherence to and implementation of the access control-policy.
6. Reports the results of key control reviews of campus departments to the Executive Vice President and Provost, at regular intervals.
7. Directs designated Facilities Management employees to establish service programs for administering, maintaining and repairing the mechanical and electronic access control systems.

3.4.2 Access Control Administrator - Associate Vice President Business Affairs, Facilities Services

Oversees the service program for access systems and is responsible for or may delegate the following items:

1. Maintaining access control files.
2. Directing the fabrication of all keys for campus spaces, mechanical access control, and specialized security keys.
3. Managing a service program for all maintenance and repair work regarding mechanical and electronic access systems.
4. Consulting with University Chief of Police (or designee) concerning records of keys lost or stolen. Decisions to re-key or to duplicate keys are based on consultation between the Chief of Police, the Access Control Administrator, and the respective Space Steward. All re-keying will be administered through the Access Control Shop. The cost of routine re-keying and key-cutting is borne by the affected Department.

3.4.4 Space Steward

The Space Steward is defined as an Executive Officer, Dean, Director or Chairperson that has been assigned those spaces through the University's formal process of space planning and allocation. The Space Steward is responsible for fully implementing this policy within their respective areas. All records are subject to review by the Vice President for Business Affairs or their delegate. Further, Internal Auditing shall perform periodic inspections of records as determined by that department.

The Space Steward's functions include the following:

1 Appointing a member of his/her department to be the Department Access Coordinator and advise, in writing, of the assigned responsibilities.
2 Responsible and accountable for the control of interior building spaces and providing access to those spaces. Therefore the Space Steward or designee must sign off on all access requests.
3 Shall exercise control of their buildings in compliance with standards and procedures established by the University.
4 Individual departments are responsible for all re-keying costs resulting from violations of this policy by their employees.

3.4.5 Campus Police

Campus Police has overarching custodial responsibility for monitoring security and responding to emergency or non-compliance of the policy for the University. Campus Police has the authority to access all areas for the purposes of fulfilling this overarching responsibility and to the extent necessary to do so, liaises with occupant units. Level II access shall be coordinated with trained personnel and Space Steward, and entry is only permitted once all the protocols as per the space specific task instructions have been fulfilled by Key Holder.

Police will also assist in coordinating emergency or security events by contacting the Space Steward or Access Control Grantor from the Facilities Management Access Control Shop to remove access as required.

3.4.6 Facilities Services Access Control Shop

The Department of Facilities Managment has overarching custodial responsibility for the operations and maintenance of the University. Facilities Management has the authority to access all Level I areas for the purposes of fulfilling this overarching responsibility and to the extent necessary to do so, liaises with occupant units and Campus Police. Level II access shall be coordinated with trained personnel and Space Steward and entry is only permitted once all the protocols as per the space specific task instructions have been fulfilled by Key Holder.

The Department of Facilities Management shall be responsible for all physical installations in University buildings that restrict access to locked space. This includes, but is not limited to doors, frames, locks, keys, door and frame hardware, electrical and fiber optic cabling, and access control hardware and devices (e.g., proximity reader, electronic strike, door contacts/magnets, electronic latches, power transfer hinge, motion sensor, etc.).

The Access Control Shop within Facilities Management shall be responsible for central key production, issuance, control of master keys, and distribution of regular/change keys to University faculties, departments and operating units.

The Access Control Shop shall:

1. Have in-staff and delegate Key Coordinators with fiduciary responsibility for the proper implementation of this SOP and management of the Access Control Systems.
2. Keep up-to-date records of an electronic key inventory
3. Keep up-to-date records on card access agreements
4. Ensure that the access policy is being followed prior to granting access to anyone
5. Ensure that all required approvals for access are obtained prior to granting access to any building
6. In conjunction with Access Granting Authorities, limit access to those individuals who have documented a need to work in the facility
7. Supply audit access reports to departments **as requested**.

3.4.7 Environmental Health and Safety (EH&S)

EH&S has overarching custodial responsibility for the safety and environmental regulatory and operational processes for the University plant, including interior building spaces. EH&S has the authority to access all Level I areas for the purposes of fulfilling this overarching responsibility and to the extent necessary to do so, liaises with occupant units and Campus Police. Level II access shall be coordinated with trained personnel and Space Steward, and entry is only permitted once all the protocols as per the space specific task instructions have been fulfilled by Key Holder.

3.4.8 All Key Holders

All Key Holders are required to:

1. Acknowledge an approved form documenting record of the issuance of the key.
2. Maintain, secure and be responsible for any access control key(s) issued,
3. Report loss or theft of access control keys to the Space Steward, and to the University Police (who will notify Facilities Management personnel) within 24 hours of discovery of theft or loss.

4. Keys must be returned to Access Control Shop, Human Resources, or mailed.

5. All Key Holders have a fiduciary duty to ensure they safeguard their access control key or card. Cards shall not be shared with any individual. Key Holders and Card Holders shall not allow piggy-backing of unauthorized persons into any space.
6. Students, faculty and staff are required to maintain and have in their immediate possession the appropriate access device (key and/or Miner Gold Card) that provides authorized access. It is each person's responsibility to maintain their Miner Gold Card on active status.
7. Visiting Scholars, Grant Appointees, Contractors, Vendors, Guests and Volunteers must apply for a Miner Gold Card and apply for access through the sponsoring Department.
8. Tampering with or attempting to bypass security on an electronically controlled or monitored door in any way, including but not limited to key bypass, propping, taping and/or dogging, is prohibited.
9. ***Those who do not follow the access protocol for these spaces will be immediately reported to UTEP Campus Police.***

3.5 - KEY LEVELS/REQUIRED AUTHORIZATIONS

3.5.1 - Building Master Key:

Building Master provides access to all Master keyed and doors with card readers in spaces to a specific building. The issuance of this key is restricted to persons authorized by the Space Steward.

3.5.2 - Building Sub-Master Key:

Building Sub-Master provides access to a group of rooms within a department or building. Authorization for this level of access will be determined by the Space Steward.

3.5.3 - Individual Room Key:

All individual keys are given to access a room/office within a specific building on campus.

Authorization is granted by the Space Steward.

3.6 CHARGEABLE/NON-CHARGEABLE KEY

3.6.1 Original Keys or Access Card:

Original keys issued to an employee are not chargeable.

3.6.2 Worn Keys or Worn Access Card:

Worn keys will be replaced without charge. Original keys must be returned to the Facilities Access Control Shop.

3.6.3 Lost or Stolen Key Replacement:

Replacement of lost/stolen keys or failure to return assigned keys will result in charges to the Department employing the person identified as the key holder. Facilities have set the following replacement costs for the various key levels:

Type of Key	Replacement Cost
Miner Gold Card	Refer to the Current Miner Gold Card Policy
Room or Outside Door Key	Dependent on mitigation cost
Building Sub-Master Key	Dependent on mitigation cost
Building Master Key	Dependent on mitigation cost

3.6.4 Lock Changes Following Lost or Stolen Key Incidents

Lock changes required to maintain building security following lost or stolen key incidents are chargeable work orders. The Building Supervisor, Dean, Director, or Department Chair will notify the Facilities Managment to have their locks rekeyed and security re-established.

In cases where re-key is recommended by the Facilities Management and/or Campus Police, the affected department(s) shall be charged the cost of re-key and any additional security measures necessary, to include but not limited to equipment and staff resources as approved by the Chief of Police or designate to ensure security of the facility during the period of time the facility is vulnerable to unauthorized entry.

3.6.5. Students Who Fail To Return Keys:

Students who fail to return keys will be subject to the same restrictions and penalties as students who fail to honor their financial obligations to the University.

3.6.6 Space Steward:

Deans, Directors or Department Chairs acknowledge keys issued by their key manager and lost or not returned could result in a charge to their department to restore security.

3.6.7 Forgotten Keys

Key holder needs to notify their respective Space Steward. Each respective Space Steward will need to open requested space. If Facilites Management is dispatched to open area a work order will be generated and billed.

3.7 KEY ISSUANCE

3.7.1 UTEP Employees:

All unclassified and classified employees may be issued keys needed to access office and/or work areas.

3.7.2 Key Request:

All key requests must be submitted via Facilities Management service desk. All key requests will be filled within three to five business days.

3.7.3 Record Management:

Facilities will maintain employee key records in its Access Control database. The Access Control Shop will provide Space Stewards with reports of key records grouped by department **as requested**, and will work with the Space Stewards to maintain the accuracy of these records as changes occur.

3.7.4 Short Term or Temporary Building Access:

For short term or temporary building access, Departments may retain duplicate check-out keys in a secured area (lockable box or cabinet). Responsibility for the security of these keys, as well as establishing a sign-out procedure to track the location of the keys, remains with the department. These temporary key storage areas will be subject to audit by the Facilities Management personnel. These keys must be issued to a Space Steward who will be responsible for their use and safekeeping.

3.7.5 Key Pick Up:

The person being assigned a University key must pick up the key in person and present their Miner Gold Card at the time of transmittal.

3.7.6 30-Day Request Period:

All keys must be picked up from the Facilities Access Control Shop within five (5) business days or the request is void and a new request will need to be submitted before a key can be issued.

3.7.7 Key or Access Card Replacement Requests:

Replacement requests for lost or stolen keys are submitted to the Space Steward. Keys will be replaced when a copy of a University Police report has been mailed/faxed/emailed to Facilities Management. The department will be charged for replacement keys.

3.7.8 Cipher Lock Management

Cipher Locks (local pin-based security systems) will be installed and maintained by Facilities Management. Pass code dissemination and recordkeeping of these systems **will** be maintained by Facilities Management.

3.8 RECORD KEEPING:

Facilities Management will keep the official records of keys issued for all University employees. Facilities will maintain a security software system which will record building key data and employee key records. Reports will be generated by the Facilities Management as requested by Space Steward.

3.9 AUDIT

1. Each Department is responsible for periodically performing physical inventories of keys, including department lock boxes.
2. The Access Control Shop will send out a list of key ID and key holders to the Space Steward annually and as requested.
3. Each Department is responsible for performing, at a minimum, annual audits of individuals who have Electronic Access to the Department space. Any changes shall be coordinated with the Space Steward and Facilities' Access Control Grantor.
4. Keys found missing at that time will be subject to **review by Campus Police and Facilites Management**

3.10 NON-UNIVERSITY LOCKS

No lock may be installed on a University building or property without the prior approval of Facilities Management. Locks installed without prior approval will be removed at the Department's expense. The cost of the unauthorized lock will not be reimbursed.

Level I Access Request Task Instruction

Task Instruction Name: Level I Access Approval Process	
Document Number: AC-001	

Overview

Purposed and Scope: This task instruction encompasses most access requests. This is to be used for Level I controlled spaces
Responsible Parties: The Space Steward is responsible for the administration of this policy within the department. The Access Control Shop is responsible only for creating keys/cards access as per authorization given on the completed form.

Procedure Steps			
Type	**Agent**	**Description**	**Deadlines**
	VPBA	Stewards responsible for approving or delegating access are designated for each space in the University.	As needed
	Space Manager	Approval routings for each space are managed via the Facilities Console, following VPBA designation and Space Stewards requests.	As needed

Trigger	Requestor	An electronic access request is submitted by the requestor via the Facilities Service Desk, including the following:
		- Contact information
		- Spaces requested
		- Recipient information
		  ○ For employees, the Active Directory username is matched with the People database extract
		  ○ For students, name, email and School ID, as well as an expiration date are requested (note: students are only eligible for electronic access to areas designated as "student accessible" by the Space Steward)
		  ○ For construction contractors, name, company and contact information, as well as an expiration date, are required (note: access for contractors is requested via the Facilities Console and must be linked to a construction project)
		- A justification and/or comments	

Automated	Service Desk	The type of access (brass key or electronic) is determined based on the space being requested. For electronic access, schedule and an expiration date (optional for recipients who are University employees) are requested.	
Automated	Service Desk	The approvers for the request are determined based on the spaces selected. - If the space has no approval routing assigned, the Space Management Office is added as the approver. The Space Management Office monitors these requests via the Facilities Console, and updates the approval routings as needed, at which point all pending requests are forwarded to the new approvers. - If any of the recipients on the request already has been assigned access to any of the spaces selected, the Space Management Office is added as an approver. The Space Manager investigates the need for a duplicate and if necessary, rejects the request or follows the appropriate procedure for lost keys. Upon submission, email notifications are sent to the requestor for tracking, the recipients and the approvers.	
	Designated Approvers	On receipt of the Service Desk email notifications, approvers access the request information via the Facilities Service Desk, where they are presented with the option to either approve or decline the request. Comments are optional for approval, but required if the request is declined.	
Automated	Service Desk	If the request is declined by the approver, an email notification is sent to the requestor including the approver's comments. The approver's username and the timestamp are recorded in the Facilities database.	
Automated	Service Desk	If the request is approved, an email notification is sent to the requestor including the approver's comments. The approver's username and the timestamp are recorded in the Facilities database. At this point the system determines If all approvals have an 'approved' status, in which case the status of the request is updated to	

		'approved' and its information is inserted into the TMA database in the form of a TMA request that is placed in the request queue.	
	Work Control	Work Control personnel reviews the request in WebTMA and accepts it. The request is then automatically assigned a work order number by the system, which is assigned to either the Key Shop and/or the Access Control Shop by Work Control.	
	Access Control Shop	The required electronic access is granted to the approved recipients in the CS Gold system, with the specified schedule and expiration date if applicable. The CS Gold system will automatically expire the access if the expiration date is specified.	
	Key Shop	If key access was requested, the appropriate key or keys for the spaces requested is selected and WebTMA is searched for an available instance of the key.	
	Key Shop	If there are no available instances of the required keys, a blank is prepared with the appropriate bitting.	
	Key Shop	The key (either pre-existing or newly created) is assigned to the client in WebTMA.	
	Key Shop	The recipient is notified via email to inform them that the key is ready and provide them with pick-up instructions, including time and place.	
	Recipient	The recipient is presented with the Key Acknowledgement interface, where they log in with their UTEP credentials and are presented with a list of brass keys assigned to them that have not been previously picked up. The recipient acknowledges receipt of the keys listed by clicking the 'acknowledge' button in the form.	
	Access Control Shop/Key Shop	The work order is completed in WebTMA, triggering an automated email notification to the requestor.	
	Service Desk	A list of keys assigned to a user is accessible to the user via the Service Desk, under 'My Profile'. Information on users with access to a space is available to the Space Steward upon request.	

Restricted Access Request Task Instruction

Document Number: AC-002	

Overview

Purposed and Scope: This task instruction encompasses access procedures to all restricted spaces on campus.
Responsible Parties: Respective Space Steward

Policies:

Id	Policy
1	**This is a restricted space. Only people with the authorization from Space Steward are allowed into the restricted area.**
2	**Before access is given, all training must be completed and documented.**
3	**All access into the restricted areas wil be monitored by each respective Space Steward.**
4	**Users shall only enter using their own credentials. Piggybacking with another user is forbidden and can result in disciplinary action up to and including termination.**
5	**Visitors shall get permission from authorized staff prior to entering and shall be accompanied by trained and authorized personnel.**