# Facilities Management

## Audit Report #16-10
## August 26, 2016

## The University of Texas at El Paso
## Institutional Audit Office

"Committed to Service, Independence and Quality"

THE UNIVERSITY of TEXAS SYSTEM
FOURTEEN INSTITUTIONS. UNLIMITED POSSIBILITIES.

UTEP Institutional Audit Office
500 West University Ave.
El Paso, Texas 79968
915-747-5191
WWW.UTEP.EDU
WWW.UTSYSTEM.EDU

August 26, 2016

Dr. Diana Natalicio
President, University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited scope audit of Facilities Management Building Access. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in the audit report. The recommendations are intended to assist the department in strengthening controls and help ensure that the University's mission, goals and objectives are achieved.

We appreciate the cooperation and assistance provided by the Facilities Services staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

# Report Distribution:

**University of Texas at El Paso:**

Mr. Richard Adauto III, Executive Vice President

Mr. Greg McNicol, Associate Vice President for Business Affairs, Facilities Management

Mr. Jesus Carrillo, Director, Facilities Services

Mr. Carlo Vazquez, Assistant Director, Facilities Services

Ms. Sandra Vasquez, Assistant Vice President for Equal Opportunity (EO) and Compliance

**University of Texas System (UT System):**

System Audit Office

**External:**

Governor's Office of Budget, Planning and Policy

Legislative Budget Board

Internal Audit Coordinator, State Auditor's Office

Sunset Advisory Commission

**Audit Committee Members:**

Mr. David Lindau

Mr. Steele Jones

Mr. Fernando Ortega

Dr. Stephen Riter

Dr. Howard Daudistel

Dr. Roberto Osegueda

Dr. Gary Edens

**Auditors Assigned to the Audit:**

Lorenzo Canales

Sharon Delgado

# TABLE OF CONTENTS

# EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Facilities Management for exterior building access controls.

During the audit we noted the following:

- The Standard Operating Procedures (SOPs) for Access Management were not posted on the Facilities Services Department website until the audit was in process. The Department of Facilities Services should work with the Department of Human Resources to recommend enforcement of the policies to the University community.
- Employees may maintain key access to buildings after they have separated from the University or transferred to another building. A judgmental sample of 15 employees with keys to the exterior doors of the Psychology Building was chosen for testing to determine if access was properly approved and still necessary. Nine (60%) of 15 employees selected no longer require keys to the Psychology Building; however, the keys were not returned to the Access Control Shop.
- Electronic access to buildings is not always terminated after an employee separates from the University or transfers to another building. A judgmental sample of 23 out of a possible 154 employees with electronic access to the exterior doors of the Administration building was chosen for testing to determine if access was properly approved and still necessary. Twenty three (100%) of 23 terminated or transferred employees tested no longer require electronic access to the Administration Building during non-business hours.
- The list of individuals having master electronic access to the exterior doors has not been reviewed or updated since 2012. Although there is no current requirement in the SOPs to do this, we recommend that a review be performed on an annual basis.
- The SOPs for Access Management state, "*The Access Control Shop will send out lists of key ID and key holders to the Department Access Coordinators on an annual basis.*" However, these lists are not sent unless requested by the Department.

Based on the results of audit procedures performed, we conclude that building access controls require coordination with Human Resources in order to communicate and recommend enforcement of the policies to help ensure the safety and security of the University community.

# BACKGROUND

Facilities Services is responsible for managing key and electronic access control systems for the University. Proper management helps ensure adequate building security as well as access to work areas by employees.

There are 69 buildings on campus. For 29 of these buildings, electronic access to the exterior doors is managed using the Miner Gold Card. The remaining 40 buildings are controlled by key access.

The Miner Gold Card is the official identification card for the faculty, staff and students of The University of Texas at El Paso. It is used to access doors controlled by a computerized card access control system using the ID number assigned to each individual. Under University policy, routine access to locked areas can be granted to employees upon proper authorization by the department. The access request form includes days of the week and the time frames when access can be granted.

# AUDIT OBJECTIVES

The objective of this audit was to analyze processes for issuing and managing University key/electronic card access to the exterior doors of campus buildings to determine if the controls in place were effective. Specifically, we audited:

- approvals for issuing building keys and electronic access to exterior doors,
- removal of building access when it no longer necessary, and the
- accuracy of records.

# SCOPE AND METHODOLOGY

The audit was conducted in accordance with the *International Standards for the Professional Practice of Internal Auditing* issued by the Institute of Internal Auditors.

Audit procedures included performing a risk analysis, reviewing University policies and procedures, interviewing key personnel and testing access approvals for a sample of employees. The scope of the audit is September 1, 2014 through March 31, 2016.

# RANKING CRITERIA

All findings in this report are ranked based on an assessment of applicable qualitative, operational control and quantitative risk factors, as well as the probability of a negative outcome occurring if the risk is not adequately mitigated. The criteria for the rankings are as follows:

**Priority** - an issue identified by an internal audit that, if not addressed timely, could directly impact achievement of a strategic or important operational objective of a UT institution or the UT System as a whole.

**High** – A finding identified by internal audit that is considered to have a medium to high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level.

**Medium** – A finding identified by internal audit that is considered to have a low to medium probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

**Low** – A finding identified by internal audit that is considered to have minimal probability of adverse effects to the UT institution either as a whole or to a college/ school/unit level.

# AUDIT RESULTS

## A. Building Access: Policies and Procedures

Policies and procedures are part of an organization's internal controls. They are used as the communication tool for guiding managers and supervisors in making decisions, training personnel and handling employment issues. Policies should be consistent across the organization to help ensure compliance.

The Office of Auditing and Consulting Services (OACS) reviewed the policies and procedures from the University Handbook of Operating Procedures (HOP), the Vice President of Business Affairs (VPBA) Business Process Guidelines (BPGs) and the Facilities Services' Standard Operating Procedures for Access Management (SOPs) internal policies related to building access management to ensure consistency and completeness with Human Resources (HR) exit procedures.

### A1. VPBA Business Process Guidelines

The BPGs on the VPBA website were outdated and no longer applicable. The link was immediately disabled and the guidelines will be updated at a later date by the VPBA office.

### A2. Policies for Removal of Access

The HOP does not address how employee access is removed when an employee transfers to a different department or separates from the University. Employee access includes both electronic access and key access.

The SOPs were drafted in 2013, and they were posted on the Access Control Shop website during the course of the audit. Consequently, they were not available to the University community for the audit period. These SOPs represent the internal policies and procedures for access control and were used for this audit.

#### SOPs Key Return

Inconsistent guidance regarding the process of surrendering keys has contributed to non-compliance with policies and inaccurate key inventory records.

The SOPs state "Key holders are required to return keys to the Department Access Coordinator, Human Resources or the Access Control Shop upon terminating from the Department." However, there are also conflicting policies on the HR website regarding the exit procedures related to where keys should be surrendered when an employee separates from the University.

### Electronic Access

When an employee separates from the University, the Miner Gold Card should be surrendered as part of the exit process. However; this does not remove an employee's access, as access is tied to the ID number, not the card. Access is not removed unless the department contacts the Access Control Shop requesting that access be removed. This procedure is not communicated to the University community. In the event the individual returns to the University in another capacity, and a new card is issued, he/she will still have access.

**Level:** This finding is considered **Medium** risk due to the fact although departments are not aware of the process for removal of building access when it is no longer needed, the individual would have limited access to interior doors.

### Recommendation:

*The HOP and SOPs should coordinate with HR to standardize procedures for the removal of access. The new policies need to be communicated to the University community.*

### Management Response:

*A newly formed position, Access Control Manager, will have the primary duties of:*

- *Ensuring adherence to established University and departmental policies and procedures, objectives, quality assurance programs and safety standards.*
- *Providing Department Access Coordinators with report of access records grouped by department as requested, and will work with the Department Key Coordinators to maintain the accuracy of these records as changes occur.*
- *Advising senior management on options and strategies for maintaining and enhancing campus-wide building security.*
- *Creating, updating, maintaining and auditing Key and Electronic access database on a continuous basis.*
- *Keeping University officials informed by preparing performance reports and communicating system status. Keeps track of personnel (active/inactive) access control status and hard key owners.*

- *Implementing security improvements by assessing current situation; evaluating trends and anticipating requirements.*

*In this role, the Access Control Manager will report directly to the Assistant Director of Research and Operations.*

**Responsible Party:**

*Mr. Carlo Vazquez, Assistant Director, Facilities Services.*

**Implementation Date:**

*March 1, 2017*

## B. Building Access Authorizations

The Access Control Shop issues keys for campus buildings upon the completion of a key request form. The key request must be approved by the Department Access Coordinator and signed by the employee.

### B1. Psychology Building (Key Access)

A list of all individuals assigned a key for the exterior doors of the Psychology building was requested from the Access Control Shop. A judgmental sample of 15 out of 58 (26%) individuals was chosen, and their key request forms were reviewed for appropriate approval with no exceptions noted. Their appointments were reviewed in PeopleSoft to determine if the individuals still required access to the building. The results are summarized in the table below:

| Number of Individuals | Percentage of Sample Tested | Status in PeopleSoft | Current Department |
|---|---|---|---|
| 8 | 53% | Inactive | Terminated |
| 1 | 7% | Active | Pharmacy |
| 6 | 40% | Active | Psychology |

9 (60%) of the 15 individuals no longer required access to the building, and the keys had not been returned to the Access Control Shop. Additionally, two of the forms reviewed had not been signed by the employee.

On the key request form, the employee certifies he/she is responsible for the safe keeping of the keys and all keys should be returned when no longer needed.

### Recommendation:

*Separated employees should return keys to the Access Control Shop prior to being cleared by Human Resources. Transferred employees should not receive new keys until all unnecessary keys have been returned to the Access Control Shop.*

**Level:** This finding is considered **Medium** due to the fact that the keys only provide access to the building and the key holder's office. This presents limited exposure to the college, school or unit.

### Management Response:

*A newly formed position, Access Control Manager, will have the primary duties of:*

- *Ensuring adherence to established University and departmental policies and procedures, objectives, quality assurance programs and safety standards.*
- *Providing Department Access Coordinators with report of access records grouped by department as requested, and will work with the Department Key Coordinators to maintain the accuracy of these records as changes occur.*
- *Advising senior management on options and strategies for maintaining and enhancing campus-wide building security.*
- *Creating, updating, maintaining and auditing Key and Electronic access database on a continuous basis.*
- *Keeping University officials informed by preparing performance reports and communicating system status. Keeps track of personnel (active/inactive) access control status and hard key owners.*
- *Implementing security improvements by assessing current situation; evaluating trends and anticipating requirements.*

*In this role, the Access Control Manager will report directly to the Assistant Director of Research and Operations.*

### Responsible Party:

*Mr. Carlo Vazquez, Assistant Director, Facilities Services*

### Implementation Date:

*March 1, 2017*

## B2. Administration Building (Electronic Access)

Access to the exterior doors of the Administration building is controlled by a computerized card access control system. A list of all individuals assigned with electronic access for the exterior doors of the Administration building was requested from the Access Control Shop.

A judgmental sample of 23 of 154 (15%) employees was chosen for testing, and their electronic access request forms were reviewed for appropriate approval. Their appointments were also reviewed in PeopleSoft to determine if the employees still required access. The results of the testing are summarized in the table below.

| Number of Individuals | Percentage Tested | Status in PeopleSoft | Reason |
|---|---|---|---|
| 8 | 35% | Active | Transferred to another department |
| 9 | 38% | Active | Relocated to another building |
| 3 | 13% | Inactive | Terminated |
| 2 | 9% | Inactive | Retired |
| 1 | 5% | Active | No longer requires access |

Per HOP, Section 8, Chapter 6.3.2 "*Electronic access to building, offices, and other facilities may only be granted to a University employee upon proper authorization by a Department.*" Failure to remove access that is no longer needed increases the risk of unauthorized admittance to University buildings.

### Recommendation:

*The HOP and SOPs should be updated and communicated to the University community to ensure compliance and awareness of responsibilities regarding building electronic access. Additionally, the Access Control Shop should reach out to Department Access Coordinators on an annual basis so that the building access lists can be reviewed for appropriateness.*

**Level:** This finding is considered **Medium risk** due to the fact that electronic access only provides access to the building, not interior doors and/or spaces. Consequently, this presents limited exposure to the college, school or unit.

**Management Response:**

*A newly formed position, Access Control Manager, will have the primary duties of:*

- *Ensuring adherence to established University and departmental policies and procedures, objectives, quality assurance programs and safety standards.*
- *Providing Department Access Coordinators with report of access records grouped by department as requested, and will work with the Department Key Coordinators to maintain the accuracy of these records as changes occur.*
- *Advising senior management on options and strategies for maintaining and enhancing campus-wide building security.*
- *Creating, updating, maintaining and auditing Key and Electronic access database on a continuous basis.*
- *Keeping University officials informed by preparing performance reports and communicating system status. Keeps track of personnel (active/inactive) access control status and hard key owners.*
- *Implementing security improvements by assessing current situation; evaluating trends and anticipating requirements.*

*In this role, the Access Control Manager will report directly to the Assistant Director of Research and Operations.*

**Responsible Party:**

*Mr. Carlo Vazquez, Assistant Director, Facilities Services.*

**Implementation Date:**

*March 1, 2017*

## B3. Master Access to Exterior Doors

A list of all individuals with master electronic access to the exterior doors was requested from the Access Control Shop. Based on interviews with the Access Control Shop, the master access has not been reviewed since 2012. There are five individuals with master access, but only one approval on file.

### Recommendation:

*The Access Control Shop should ensure that the proper approvals are maintained and on file for master electronic access, and the requirement for approval and documentation added to the current SOPs. Additionally, these approvals should be submitted for review on an annual basis to ensure appropriateness.*

**Level:** This finding is considered **Medium** as there is limited exposure due to the small number of individuals possessing master access.

### Management Response:

*Policy will be updated to reflect a requirement for approval for master electronic access and documentation of the approval.*

### Responsible Party:

*Mr. Carlo Vazquez, Assistant Director, Facilities Services.*

### Implementation Date:

*March 1, 2017*

### C. Building Access Monitoring

## C1. Access Audit

Section 3.9 Audit of the Standard Operating Procedures states, "*The Access Control Shop will send out a list of Key ID and key holders to the Department Access Coordinators on an annual basis.*"

The Access Control Shop does not send out yearly lists detailing the individuals with electronic access and/or key holders to the Department Access Coordinators unless requested. Failure to monitor access increases the risk of unauthorized individuals having access to University buildings.

### Recommendation:

*The Access Control Shop should coordinate with the departments and send the access reports to the Department Access Coordinators on an annual basis.*

**Level:** This finding is considered **Medium** as although individuals may have access to the exterior doors, this does not guarantee access to interior doors and/or spaces. Consequently, this presents limited exposure to the college, school or unit.

### Management Response:

*A newly formed position, Access Control Manager, will have the primary duties of:*

- *Ensuring adherence to established University and departmental policies and procedures, objectives, quality assurance programs and safety standards.*
- *Providing Department Access Coordinators with report of access records grouped by department as requested, and will work with the Department Key Coordinators to maintain the accuracy of these records as changes occur.*
- *Advising senior management on options and strategies for maintaining and enhancing campus-wide building security.*
- *Creating, updating, maintaining and auditing Key and Electronic access database on a continuous basis.*
- *Keeping University officials informed by preparing performance reports and communicating system status. Keeps track of personnel (active/inactive) access control status and hard key owners.*
- *Implementing security improvements by assessing current situation; evaluating trends and anticipating requirements.*

*In this role, the Access Control Manager will report directly to the Assistant Director of Research and Operations.*

### Responsible Party:

*Mr. Carlo Vazquez, Assistant Director, Facilities Services.*

### Implementation Date:

*March 1, 2017*

# CONCLUSION

Based on the results of audit procedures performed, we conclude that building access controls require revisions to help ensure the safety and security of the University community.

We wish to thank the management and staff of Facilities Services for their assistance and cooperation provided throughout the audit.