Office of Internal Audit Services

UT Southwestern
Medical Center

Physical Access Audit

Internal Audit Report 22:11

April 1, 2022

Table of Contents

Executive Summary

Background

Physical access pertains to the management of access control points into UT Southwestern (UTSW) operated facilities and work areas across the UT Southwestern campus and in UT Southwestern leased spaces. Physical entry is variable through centrally monitored electronically scanned badges, physical keys and decentralized battery powered entry devices (BPED) or keypads requiring separate codes. All UT Southwestern students, employees, faculty members and approved persons must wear institution issued identification (ID) badges whenever they are on campus to promote overall safety by identifying parties who belong on campus. Additionally, UT Southwestern Police Officers and Public Safety personnel are deployed throughout the main campus and off-campus to enhance the overall safety and security.

The Access Control team reporting to the University Police Department (UPD) is responsible for issuing and managing all ID badges, access-control points, and the campus-wide video management system for certain perimeter entrances or high-security locations. The UPD Access Control team uses the Lenel System to manage ID badges, including badge issuance, access right activation and deactivation, and monitoring of facility access points.

The Facilities Management Department Building Maintenance & Operations Division (Facilities) is responsible for issuing and managing keys and installing keypads in individual offices at all UT Southwestern facilities. Facilities uses the Archibus Facilities Management and Space Planning System to issue keys upon department request, replace and recover keys. Employee records are maintained in PeopleSoft HCM and student records are maintained in PeopleSoft Campus Solutions. These system modules provide daily updates of new hires, transfers and terminations as part of interface with Lenel and Archibus. There are 37,495 active badges in the Lenel database.

Scope and Objectives

The Office of Internal Audit Services has completed its Physical Access audit. This was a risk-based audit and part of the fiscal year (FY) 2022 Audit Plan. The audit scope included physical access to facilities and buildings including badges, keys, and keypad records for fiscal year (FY) 2021 and the first three months of FY 2022 for campus and off-campus locations. The scope included facility badge and key access systems. UPD camera monitoring, campus patrols and incident responses were not in scope. The objectives were to assess the adequacy and effectiveness of controls in place to ensure:

- Physical access controls are effective to promote overall safety and security across UTSW operated facilities.
- Process for granting and managing physical access aligns with employee’s need for having access to a location.
- Physical access oversight and monitoring processes and controls are effective.
- Physical spaces requiring special access follows policies, procedures, and regulations.

Executive Summary

Conclusion

Physical access to the UT Southwestern community is a shared risk that is managed through the University Police, Facilities Management, Human Resources and Departments. While there have been physical access assessments performed by the University Police, an overall comprehensive physical access risk assessment needs to be performed for on campus and off-site locations to identify all physical access entry points, establish risk criteria for high security and sensitive areas and access requirements for the various types of space. This collaborative risk assessment would ensure appropriate physical access to all on-site and off-site locations where UT Southwestern employees work to reduce unauthorized access or safety risks. In addition, external building entry points are now restricted to not allow access to everyone, but only to those with badge access to those buildings. Opportunities also exist to improve processes and monitoring controls to ensure keys and badges are returned and badge access is updated or deactivated timely for terminated employees, employee transfers and non-UT Southwestern employees such as vendors and visitors. Strengthening the processes and controls would also help to ensure employees and non-UT Southwestern employees have the appropriate access that aligns with physical access requirements. Leadership is implementing Employee Experience Center initiative to enhance employee experience when beginning employment or leaving UT Southwestern. As part of the initiative, Human Resources will have dedicated areas for badge issuance and return. Having more locations for employees to turn in their badges coupled with creating reports for monitoring badge returns will reduce the number of badges that are not returned to UT Southwestern. Leadership is also initiating the Identity Access Management project to have a comprehensive program to manage access and identity integration for all systems across the institution, which would ensure the right users have the appropriate access to systems and technology.

Included in the table below is a summary of the observations along with the respective disposition of these observations within the UT Southwestern internal audit risk definition and classification process. See Appendix A for Risk Rating Classifications and Definitions.

Priority (0)	**High (0)**	**Medium (4)**	**Low (0)**	**Total (4)**

Key observations are listed below.

- ● **#1. Implement a Campus-Wide Comprehensive Physical Access Risk Assessment** - Assessments are done periodically as physical security concerns may arise. However, a formal campus-wide physical access risk assessment has not been performed to assess physical access risk exposure for unauthorized access and establish criteria for level of access to these spaces to determine appropriate physical access needs on campus and off campus including leased locations.

Executive Summary

- **#2. Strengthen Processes and Controls to Remove Physical Access for Terminated Employees and Internal Transfers** - Controls need to be improved to ensure physical access is terminated or updated when employees are terminated voluntarily or transfer to another department.
- **#3. Improve Badge Access Process and Accountability for Non-UT Southwestern Persons** - Physical access process needs improvement to ensure appropriate access for non-UT Southwestern persons including issuance of badge and duration of work performed at UT Southwestern locations.
- **#4. Enhance Physical Access System Data and Monitoring Effectiveness** – Physical access data reporting is not current or not available to allow for more efficient and effective access monitoring and updating of employee and non-employee access.

We would like to take the opportunity to thank the individuals included in this audit for the courtesies extended to us and for their cooperation during our review.

Sincerely,

Valla F. Wilson, Vice President and Chief Audit Executive, Office of Internal Audit Services

Audit Team:

Angeliki Marko, Internal Audit Manager
Van Nguyen, Internal Audit Supervisor
Mia Dinh, Internal Auditor II
Uzoamaka Okafor, Internal Auditor II

cc: Raymond Chow, Director, Technical Services, IR-AAIR Administration
Ann Chisholm, Project Manager, Human Resources Administration Office
Holly Crawford, Executive Vice President, Business Affairs
Archana Cronjaeger, Assistant Vice President, Hospital Facilities – Clements University Hospital Operations
Kyle Dykes, Manager, Facilities Management, Building Maintenance, Building Maintenance Administration
Suzanne Farmer, Assistant Vice President, Organizational Development & Training
Matthew Fulgham, Director, Real Estate Services
Barvette Garrett, Director, Employee Relations, HR Employee Relations
Juan Guerra, Vice President, Facilities Management

Executive Summary

Keith Herl, Manager Talent Acquisition, HR Talent Acquisition
Stephen Lawson, Director, Real Estate Services
Jodi Levy, Assistant Vice President, Administrative Systems, IR-AAIR Administration
Marcus Lewis, Chief of Police, University Police
Nathan Mason, Director, Academic Administration Data Services, IR Enterprise Data Services
Joshua McKean, Senior Manager, Access Control, University Police
Robert McMullen, Director Health System Data Services, IR Enterprise Data Services
Heather Mishra, Associate Vice President, Academic & Administrative Information Systems, IR-AAIR Administration
Adolfo Ortuzar, Assistant Vice President, IR Constituent Experience and Compliance, IR-AAIR Administration
Russ Poole, Vice President & Chief Information Officer, Information Resources
Natalie Ramello, J.D., Vice President, Institutional Compliance, Office of Compliance
Sara Rasmus, Assistant Vice President, HR Strategic Initiatives
Sudhakar Reddy, Senior Manager, Information Resources, IR-AAIR Administration
Orlando Salazar, Assistant Director, Building Maintenance, Building Maintenance Admin
Michael Serber, Vice President, Finance and Institutional Chief Financial Officer, Financial Affairs
Melissa Sotelo, Supervisor, Talent Navigator, HR Talent Acquisition
Billy Talkington, University Police Captain, University Police
Sherri Toney, Assistant Vice President Employee Relations, HR Employee Relations

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **1. Implement a Campus-Wide Comprehensive Physical Access Risk Assessment** Assessments are done periodically as physical security concerns may arise. However, a formal campus-wide physical access risk assessment is not performed to evaluate physical access risk exposure for unauthorized access and establish criteria for access level to these spaces to determine appropriate physical access needs. While there are high-security and sensitive physical locations such as research, labs, pharmacy and computer server locations, there are no established criteria to define high security locations to gain access to the spaces, and it is left up to the departments to maintain the access. A comprehensive listing of high-security locations is not available for more robust overall campus physical access monitoring. UPD manages badge access and monitors existing camera and alarm systems. There is risk of unauthorized access and possible exposure or safety issues without having a defined physical access and risk exposure assessment and plan. Physical access also varies for UT Southwestern operated facilities leased from external entities, such as off-site clinics and administrative offices.	1. Consider a workgroup led by UPD and Facilities and include representation from key stakeholders from the institution to identify a list of the access points and assess risk factors for physical access to campus and off-campus facilities. Implement plan steps or measures to mitigate high risk areas associated with facilities access. 2. Based on the risk assessment, establish institutional criteria to help determine high-security and sensitive physical locations. Document a comprehensive listing of high-security locations to facilitate more focused monitoring. 3. Review physical access risk assessment for any major changes such as new locations on an annual basis. 4. Include off-site leasing space physical access in the access risk assessment to determine if additional physical access requirements are needed and whether UT Southwestern leased spaces provide the level of security needed for its employees. 5. Determine action plan to address any critical physical access control areas and recommendations for future contractual agreements for leased spaces.	***Management Action Plans:*** 1. UPD and Facilities: We will develop a work group to include Real Estate, Business Continuity, IR, Human Resources, Business Affairs, Academic Affairs, Health System Affairs and others as needed. We will develop a preliminary listing of the physical internal and external access points of high risk areas on campus and off campus. 2. Based on key stakeholders' input, we will determine risk criteria to be used to determine high security or sensitive locations to include internal and external entry points 3. We will make updates to the assessment periodically as we add new locations or modify space use in existing locations. 4. We will work with leasing sites department points of contact and Real Estate to assess security concerns/vulnerabilities and recommend solutions. 5. We will assess future leased spaces and make security recommendations and provide the recommendations to Real Estate. 6. We will review the policy FSS-312 and determine content updates for the leased locations. ***Action Plan Owner(s):***

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
Physical access and security controls may be dependent on the building owners based on contractual agreement and UPD does not directly administer Lenel access control in all cases. For example, UT Southwestern non-UPD personnel (project manager) administer Lenel badge access control for a leased location including verifying requesters' identity, printing and issuing badges, updating user records, and performing monitoring duties. Lack of central oversight increases the exposure of unauthorized physical access to UT Southwestern leased locations and untimely mitigation of any adverse events.	6. Update Policy FSS-312 to include access control responsibility over UT Southwestern operated leased facilities. Consider having UPD Access Control to expand responsibility over the Lenel badge access administration for off-site, locations equipped with such devices.	*1-5.* Chief of Police Senior Manager, Access Control, University Police Vice President of Facilities Management 6. Chief of Police Vice President of Facilities Management ***<u>Target Completion Dates:</u>*** *1. July 31, 2022* *2. September 30, 2022* *3. October 30, 2022 and ongoing afterwards* *4. July 31, 2022* *5. August 30, 2022* *6. November 30, 2022*

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **2. Strengthen Processes and Controls to Remove Physical Access for Terminated Employees and Internal Transfers** Controls need to be improved to ensure physical access is terminated or updated when employees terminate voluntarily or transfer to another department. Process and control opportunities include the following: - Current policies and procedures require employees to turn in badges and keys to the HR front desk rather than the supervisor retrieving the badge or keys. There are no consequences or formal reporting when badges and keys are not turned in. Per data analytics of Orbit Facilities Keys Details Report, as of December 2021, there were terminated employee records with active keys (1,483). When departments do not report employee changes to Facilities, keys may inappropriately remain in possession of terminated employees. While badge access may be deactivated but not retrieved, physical safety could be compromised if persons inappropriately gained access by showing badges or using keys to gain entry to areas.	1. HR: Reemphasize with departments to have the separating employees return keys and badges promptly to HR front desk or their supervisors who will return to HR. Add options of returning badge and keys through mail for remote workers in the Separation Process checklist. 2. HR: Consider implementing consequence measures for employees not returning keys and badges upon separation such as imposing fees or delaying vacation accrual payout as is done in other cases. 3. UPD: Follow up with IR PeopleSoft and Lenel Support to ensure system interface from HCM to Lenel and Lenel scripts are functioning as intended for terminated employees. 4. UPD and Facilities: Generate reports and provide to the departments to perform periodic reviews of active keys and badges assigned to their personnel as part of their annual space assignment and update results with Facilities and UPD. We will educate departments about the available reports.	**Management Action Plans:** 1. We will reinforce the policy EMP 452 Employee Separation Requirements for returning badges and keys to HR or to the supervisor. 2A. We can perform an analysis whether it is cost effective to implement processes to ensure all physical badges are returned. 2B. We can perform an analysis whether it is cost effective to implement processes to ensure all keys are returned. 3. We will work with HR and Lenel to develop a more robust Lenel/PeopleSoft interface with features to address new hires, transfers and terminations. 4. Facilities will coordinate with EDW team to ensure the Orbit report HCi057 and other relevant reports for keys are available to all departments to be downloaded for review and update with Facilities Management. Facilities will work with institutional management to require self-audit of keys and badges annually. UPD is working with the EDW team to develop a Power BI Orbit report to accurately capture cardholder data to include employee ID. We will explore options with Lenel on implementing an advanced reporting module. We will include the links to the reports in the employee separation checklist.

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
- Termination transactions appropriately processed in PeopleSoft HCM, interface automatically with the Lenel system for daily badge access deactivation. However, badges are not always deactivated. Testing identified eleven badges assigned to terminated employees out of a subset of 27 records and five badges assigned to inactive students out of 20 records. The root causes include PeopleSoft/Lenel interface issue, Lenel processing errors, and Lenel script errors. - Transferred employees still have badge and key access to prior departments. There is no formal process for departments to notify Access Control to deactivate badge access and retrieve keys when employees no longer need access to the physical areas related to their former job duties. The transferring departments have to request an access update for employee transfers, but the previous position's physical access may not necessarily be deactivated. - Battery Powered Entry Devices (BPED) and keypads are not centrally tracked and departments are responsible for managing the access codes. Risk of inappropriate entry exists since the departments do not always change the keypad code when employees no longer work for the department.	5. HR: Develop a checklist for Employee transfers to ensure employee physical access is updated and keys are retrieved before employees start new assignments in new departments. UPD: Consider developing an automated script on Lenel to deactivate badge access when employee transfer transactions are processed. 6. Facilities: Appoint management members to perform a cost/benefit analysis and recommend options for improved administration over BPED to include centralized administration and/or leverage existing technology or introduce new technology. Consider having a robust approval process for BPED requests beyond department heads. Inclusion of UPD as approvers would help ensure BPED are not installed in high-security areas.	5. A. We will create the checklist for transfers to incorporate the needed steps for badge access removal and returning keys. 5. B. We will explore the feasibility of using a Lenel module to establish an automated process for granting/removing badge access for new hires and transfers. Continue to manually verify automated daily reports of terminated employees to ensure that the system interface is functioning properly. 6. Facilities modify FSS 312 to include oversight of BPED to provide clear guidelines on where they can be installed, what they access, and keypad code governance, and periodic code changes. Approval process for BPED requests beyond department heads. **Action Plan Owner:** 1. Assistant Vice President of Human Resources and Strategic Initiatives 2A. Assistant Vice President of Human Resources and Strategic Initiatives 2B. Assistant Director, Building Maintenance 3. Senior Manager, Access Control, University Police Senior Manager, Information Resources, IR-AAIR Administration

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
Departments are not required to periodically review badge access and key assignment reporting as a detective control to ensure appropriate access to physical areas under assigned department staff responsibilities.		4. Senior Manager, Access Control, University Police Assistant Director, Building Maintenance 5.A. Supervisor, Talent Navigator, HR Talent Acquisition Assistant Vice President of Human Resources and Strategic Initiatives 5.B. Senior Manager, Access Control, University Police 6. Assistant Director, Building Maintenance **<u>Target Completion Dates:</u>** 1. June 30, 2022 2A. June 30, 2022 2B. June 30, 2022 3. August 31, 2022 to evaluate the system scripts for terminated and transfers. December 31 to updated system features. April 30, 2023 to implement updated scripts 4. September 30, 2022 5. July 31, 2022 6. July 31, 2022

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
Risk Rating: Medium ● **3. Improve Badge Access Process and Accountability for Non-UT Southwestern Persons** Processes and controls need to be strengthened to reduce risks of non-UT Southwestern persons from having inappropriate access to facilities. When departments need contractors or vendors to gain physical access to facilities, the sponsoring department management is required to complete a non-employee application form and send the non-employee to the UPD to obtain badge. The form does not capture key information which should be provided such as business purpose, expiration date for badge activations, or acceptable forms of ID. UPD verifies the applicant's identity on the pictured ID card presented but does not scan in a copy of the card as support for the badge issuance. Since departments do not always enter the expiration date on the non-employee request form, there is a risk access is granted for an extended period or indefinitely after the assignment or services end. There is also no formal process for departments to notify UPD of badge holders' subsequent transfer activities or location changes. Testing identified the following: • The Lenel database has badge access types for new account setup with default expiration dates ranging from 5 days to 99 years. These serve as guidelines during manual account setup and subsequent maintenance only rather than hard system controls.	1. UPD: Coordinate with Lenel Support to revamp the current types of access badges and appropriate expiration timeframes to ensure reasonableness and consider default for those not identified or requiring departments to define the period similar to system access. Consider implementing Lenel system controls to ensure expiration and termination to mitigate risk for unauthorized badge access. 2. Coordinate to determine revamped information requirements for non-employee badge requests and required supporting documentation. Consider making business purpose and expiration date mandatory fields for non-employee ID badge application forms. 3. Implement process for providing reports and requirements for department sponsors to perform periodic reviews of the non-UT Southwestern employees badge access to ensure current access is valid.	**Management Action Plans:** 1. We will review and make appropriate modifications to expiration dates for all badge types. 2. We will require expiration dates on badge application form for badge issuance for contractor/visitors. 3. We will run annual reports and provide to department sponsors to cross-reference with approved campus contractors. **Action Plan Owner:** Senior Manager, Access Control, University Police **Target Completion Dates:** 1. January 31, 2023 2. June 30, 2022 3. September 30, 2022

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
• Active badges with generic names under HR Employee badge type were issued to contractors and visitors (11) making it difficult to determine identity of badge holders increasing the risk of people being granted inappropriate badge access. Active badges were issued for Person of Interest (POIs) (4) that never started work at UT Southwestern.		
Risk Rating: Medium ● **4. <u>Enhance Physical Access System Data and Monitoring Effectiveness</u>** System data for reporting of physical access types is not current or available and reporting is not used for effectively monitoring access. Key reporting issues include: • The Lenel system does not have reports available with relevant data fields such as badge holders' employee ID number, position description, and department for monitoring purposes. • Per data analytics of Orbit Facilities Keys Details Report, Archibus system keys transaction details include 80 cases of active keys assigned to two different employees with the same key identifiers and 256 employees without key identifiers.	1. UPD consider leveraging additional monitoring reports to ensure timely and appropriate Lenel badge access status. 2. Facilities: Develop a plan and allocate resources to update the Archibus database including resolving and closing out outstanding key records data correction in Archibus. 3. Hospital Facilities: Develop a plan to manage Zale Pavilion key records in Archibus and designate a backup for the locksmith position. Review and close out open work orders at the earliest practical. Reemphasize more frequent reviews of system aging report.	**<u>Management Action Plans:</u>** 1. We are working with the EDW team to develop a Power BI Orbit report to accurately capture cardholder data to include employee ID. We will explore options with Lenel on implementing an advanced reporting module. 2A. Facilities will review the Archibus system and develop a plan and funding request to update the application to address system deficiencies for executive approval and tracking. 2B. Facilities will reissue keys to employees who have duplicate key identifiers. Facilities will contact employees to reissue new keys with key identifiers and recover old keys that do not have key identifiers. 3 A. We are in the process of creating a new key tree for Zale. We are still in the design phase.

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
This increases risk of inability to track keys. An Archibus system programming glitch contributed to these issues. • Zale Pavilion employee key records are maintained manually through a spreadsheet outside Archibus solely by the hospital locksmith without a backup person. • Orbit Hospitals Work Order (WO) Aging Report contained dated open key service requests ranging up to several years old, which impacted reporting accuracy, efficient and effective monitoring.		3B. As soon as the key tree is approved and we get the funding, we will change the hardware and issuing new keys to everyone at Zale. All this will be implemented into Archibus as it is at CUH. 3C. We have designated a backup for the locksmith position. 3D. The referenced work orders were closed prior to the completion of the audit **Action Plan Owner:** 1. Senior Manager, Access Control, University Police Director, Academic Administration Data Services, IR Enterprise Data Services 2. Assistant Director, Building Maintenance 3. Assistant Vice President, Hospital Facilities **Target Completion Dates:** 1. September 30, 2022 2A. December 1, 2022 Zale key tree design

Detailed Observation and Action Plans Matrix

Observation	Recommendation	Management Response
		2B. April 30, 2023 for replacing all the blank and duplicate keys 3A. June 30, 2022 - Zale key tree design and approval 3B. September 30, 2022 – Obtain funding December 31, 2022 – Implement Zale key tracking in Archibus 3C. Completed - Designated backup person 3D. Completed - Closed out open WOs

Appendix A – Risk Classifications and Definitions

As you review each observation within the Detailed Observations and Action Plans Matrix of this report, please note that we have included a color-coded depiction as to the perceived degree of risk represented by each of the observations identified during our review. The following chart is intended to provide information with respect to the applicable definitions and terms utilized as part of our risk ranking process:

Risk Definition- The degree of risk that exists based upon the identified deficiency combined with the subsequent priority of action to be undertaken by management.	**Degree of Risk and Priority of Action**	
	Priority	An issue identified by Internal Audit that, if not addressed immediately, has a high probability to 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 high probability of adverse effects to the UT institution either as a whole or to a significant college/school/unit level. As such, immediate action is required by management in order to address the noted concern and reduce risks to the organization.
	Medium	A finding identified by Internal Audit that is considered to have a medium probability of adverse effects to the UT institution either as a whole or to a college/school/unit level. As such, action is needed by management in order to address the noted concern and reduce the risk to a more desirable 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. As such, action should be taken by management to address the noted concern and reduce risks to the organization.

It is important to note that considerable professional judgment is required in determining the overall ratings presented on the above pages of this report. Accordingly, others could evaluate the results differently and draw different conclusions. It is also important to note that this report provides management with information about the condition of risks and internal controls at one point in time. Future changes in environmental factors and actions by personnel may significantly and adversely impact these risks and controls in ways that this report did not and cannot anticipate.