UTHealth
The University of Texas Health Science Center at Tyler

Office of Internal Audit

February 5, 2021

Dr. Kirk A. Calhoun, President
UT Health Science Center at Tyler
11937 U. S. Hwy 271
Tyler, TX 75708

Dr. Calhoun,

We have completed the Employee Off-Boarding Audit that was part of our Fiscal Year (FY) 2021 Audit Plan. The objective of this audit was to assess the current processes and controls in place, post-implementation of the new Institutional policy, for the timely and accurate removal of UTHSCT employee access as the result of termination and/or transfer. This audit will meet the biennial Texas Administrative Code (TAC) §202.76 risk-based review of compliance with Texas information security standards. The scope of the audit was from March 1, 2020 through November 6, 2020 for UT Health Science Center at Tyler.

This audit was conducted in accordance with guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing.* We appreciate the assistance provided by everyone we worked with on this audit and hope the information presented in our report is helpful.

Sincerely,

Stephen Ford
Vice President, Chief Audit Executive

Enclosure
cc:
Mr. Joe Woelkers, Executive Vice President, Chief Operating and Business Officer joe.woelkers@uthct.edu
Ms. Kris Kavasch, Senior Vice President, Finance & Chief Financial Officer kris.kavasch@uthct.edu
Ms. Cindy Scott, Senior Vice President, Human Resources & Chief Human Resources Officer cindy.scott@uthct.edu
Mr. John Yoder, Vice President, Information Technology & Chief Information Officer john.yoder@uthct.edu
Mr. Robert Cromley, Chief of Police robert.cromley@uthct.edu
Mr. Paul Modisette, Director of Information Security paul.modisette@uthct.edu
Ms. Monetta Schwartz, Director of Information Technology monetta.schwartz@uthct.edu
Ms. Kimberly Griffin, Director of Human Resources kimberly.griffin@uthct.edu
Mr. Jared Seigler, Director, Human Resources jared.seigler@uthct.edu
Mr. Leonard Mayo, Police Lieutenant leonard.mayo@uthct.edu

Dr. John M. Zerwas, UT System Executive Vice Chancellor for Health Affairs jzerwas@utsystem.edu
Mr. Patrick Francis, UT System Associate Vice Chancellor for Health Affairs pfrancis@utsystem.edu
Mr. J. Michael Peppers, UT System Chief Audit Executive systemauditoffice@utsystem.edu
Ms. Dyan Hudson, UT System Director of Specialty Audit Services dhudson@utsystem.edu
Legislative Budget Board audit@lbb.state.tx.us
Governor budgetandpolicyreports@gov.texas.gov
State Auditor's Office iacoordinator@sao.state.tx.us

Employee Off-Boarding Audit

February 5, 2021

UT HEALTH SCIENCE CENTER AT TYLER
OFFICE OF INTERNAL AUDIT
11937 US HIGHWAY 271
TYLER, TX 75708

TABLE OF CONTENTS

Report

Background

The Employee Off-Boarding Audit was completed as part of the Fiscal Year (FY) 2021 Audit Plan as a risk-based audit. This area was previously audited in FY 2019 and the testing focused on the Institution's compliance with best practices. As a result of the previous audit, UT Health Science Center at Tyler (UTHSCT) implemented an Institutional policy governing this area.

It is important to note for this audit that the employee off-boarding process is comprised of both terminated employees (voluntary and involuntary) and employees who transferred departments within the Institution.

As we noted in the background of the previous audit in this area, in 2017 OneLogin, an identity management company, conducted a survey completed by 500 Information Technology (IT) decision makers in the United States. The survey revealed that nearly half of the respondents (48%) were aware of former employees who still had access to corporate applications. In a recent survey they conducted in this area, 1 in 20 organizations reported they have no way of telling whether people who left their organization still had access. 20 percent of the respondents reported that failure to deprovision employees from corporate applications contributed to a data breach at their organization. In another survey they conducted, over 13 percent of people reported they could still access a previous employers' systems using their old credentials. OneLogin notes that the impact of a breach for companies on average costs $148 per record and $7.91 million per breach in the U.S.

In a 2020 Forbes article on cybersecurity risks associated with improper employee off-boarding, it points to a former IT administrator at a boot manufacturing company who was fired and retaliated against the company before his access was removed. According to the article he shut down servers, deleted files and damaged the company network. The individual worked quickly and had done significant damage within an hour of his termination.

Currently, each departing UTHSCT employee has an electronic notification email initiated in the system when the Human Resources (HR) Department processes their termination Personnel Action (PA) form. Several departments, including HR, the Police Department, IT, and Payroll are included on this notification email. Each department is responsible for ensuring that certain actions, such as access removal and the discontinuation of all compensation, are completed in a timely manner.

Objective

The objective of this audit was to assess the current processes and controls in place, post-implementation of the new Institutional policy, for the timely and accurate removal of UTHSCT employee access as the result of termination and/or transfer. This audit will meet the biennial Texas Administrative Code (TAC) §202.76 risk-based review of compliance with Texas information security standards.

Scope and Methodology

The scope of the audit was from March 1, 2020 through November 6, 2020 for UTHSCT.

To achieve the audit objective, we:

- Reviewed applicable regulations, guidance and UTHSCT policies;
- Performed a walkthrough of employee off-boarding procedures at each department that is part of the standard employee check-out process; and
- Selected a sample of terminated employees and a sample of employees who transferred departments in order to review their applicable exit documentation and digital profile.

The audit was conducted in accordance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*.

Audit Results

We selected a total of 51 employees for testing; 16 employees who were identified as terminated for cause, 25 employees who were identified as terminated not for cause (including Reduction in Force (RIFs)), and 10 employees who were identified as interdepartmental transfers on the reports provided to us by HR.

We answered the following six (6) questions for each of the sampled employees:

1) Was the terminated or transferred employee's network access (applications authenticated through the Active Directory (AD), which comprises the Institution's highest risk systems) disabled or changed timely (20 exceptions, inclusive of 10 exceptions where we were unable to make a determination due to a lack of supporting information);

2) Were the terminated or transferred employees' miscellaneous accounts (all other applications not authenticated through the AD) disabled or changed timely (51 exceptions, each exception resulting from being unable to make a determination due to a lack of supporting information);

3) Was the terminated or transferred employee's physical access disabled or changed timely (29 exceptions);

4) Was the terminated or transferred employee's state-owned property collected in a timely manner (51 exceptions, each exception resulting from being unable to make a determination due to a lack of supporting information);

5) Was the terminated employee's final paycheck processed timely (0 exceptions); and

6) Were the terminated employee's benefits disabled timely (0 exceptions).

Findings and Recommendations

Issue #1: Currently, Institutional policies relating to the employee off-boarding process do not specify a separate timeline for employees terminated for cause.

Recommendation #1: UTHSCT should consider requiring immediate account deactivation and collection of Institutional equipment for employees terminated for cause.

Ranking: High

Management's Response: Current policy addresses voluntary resignations. For terminations for cause, HR will draft department Standard Operating Procedures (SOPs) and guidelines on the HR Shared drive for department leaders. Requirement will be to immediately deactivate employee account (PA) and notify department leader in writing to collect UT property and step by step procedures. HR will add off-boarding to the existing "101 Manager" training module.

Implementation Date: April 1, 2021

Issue #2: As part of our testing, we noted untimely account deactivation and unreturned badges and/or keys for numerous terminated and transferred employees. It should be noted that the untimely account deactivations identified were as a result of untimely PA submissions by department managers.

Recommendation #2: HR, in coordination with IT and the current off-boarding notification process, should develop a digital check-out form to be completed by the department manager to help ensure that all employee access is deactivated, and equipment is returned in a timely manner upon termination or transfer. HR should continue training efforts to help ensure that department managers are submitting PA forms in a timely manner.

Ranking: High

Management's Response: Agreed. Employee Exit Checkout list exists on the HR Shared drive. HR will develop a standard procedure upon notification of a termination for leaders to inform terminating employees to print the Employee Exit Checkout form and submit electronic termination PA, and submit the form prior to their last day of employment. This form will be required by all terminating employees.

Implementation Date: March 1, 2021

Issue #3: Currently, UTHSCT does not have a complete inventory list of all system applications utilized at the Institution.

Recommendation #3: IT should ensure that a complete and accurate system application inventory list is finalized and utilized as part of the employee off-boarding and transfer processes. In addition, IT should consider developing a role-based system access process, inclusive of all applications, to help ensure all system access is deactivated or modified as part of the employee off-boarding and transfer processes.

Ranking: High

Management's Response: Agreed. A role-based access system is an acceptable solution. However, this is dependent on the way data is entered into PeopleSoft (positions). If position management is accurately utilized, then we could identify applications and associated security profiles needed for each position. Based on the application "list", we automatically alert the Data Owner (DO) with all related on-boarding and off-boarding activities and bypass much of the existing security form process. Depending on the specific application, the security setup could also be automated with a script. The software checklist process led by Information Security will have to change in order to accommodate this type of setup.

Implementation Date: Plan for Process Implementation: June 30, 2021

Initial Pilot Implementation: December 31, 2021

Issue #4: Currently, UTHSCT does not have a consistent process in place to ensure that all applicable system access changes are completed and captured on an auditable log.

Recommendation #4: IT should develop and implement a consistent process that will help ensure all applicable system access is deactivated or modified and can be tracked effectively.

Ranking: High

Management's Response: Agreed. IT is currently evaluating new helpdesk automation software (ServiceNow) that will consolidate the security forms into a single helpdesk/ticketing/requesting/automation service.

Implementation Date: December 31, 2021

Issue #5: Currently, UTHSCT does not have a complete and accurate IT asset inventory.

Recommendation #5: IT should ensure that a complete and accurate IT asset inventory is developed and utilized as part of the employee off-boarding and transfer processes.

Ranking: High

Management's Response: Agreed. ServiceNow will manage assets as they are distributed for use. This is a manual uplift and while it could start this year (assuming ServiceNow is approved), it would take time to fully load. This would not be the official state inventory as official inventory is stored in PeopleSoft Financials.

Implementation Date: December 31, 2021

Issue #6: Currently, UTHSCT does not have a formal notification process for interdepartmental transfers.

Recommendation #6: HR, in coordination with IT, should develop a notification process for interdepartmental transfers so that all applicable departments are notified to ensure that employee access is deactivated or modified, and necessary equipment is returned in a timely manner upon transfer.

Ranking: Medium

Management's Response: Agreed. Current process is for department leaders to notify IT of an employee no longer being eligible for access to a specific account or specific equipment. HR will revise the Exit Checkout form to include transfers.
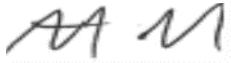
Implementation Date: April 1, 2021

Conclusion

Our audit identified areas where the employee off-boarding controls and processes in place at UTHSCT could be strengthened. We found inconsistencies in the processes for assuring removal of employee access upon termination or transfer. We also noted inconsistencies in the timeliness

of removing employee access in the areas tested. The above recommendations have been made to improve these areas.

_____

Stephen Ford
Vice President, Chief Audit Executive