UT San Antonio™
The University of Texas at San Antonio

Office of Internal Audit & Consulting Service
7703 Floyd Curl Drive MC#7974
San Antonio, Texas 78229-3900
210-567-2370

Date: February 12, 2026

To: Andrea Marks, Senior Executive Vice President & Chief Operating Officer

From: John Lazarine, Associate Vice President & Chief Audit Executive
Internal Audit & Consulting Services

Subject: Audit Report – *Offboarding Audit Report*

As part of the FY 2025 academic campus Audit Plan, we completed an audit of Offboarding Process. Attached is the report detailing the results of this review. Management's Action Plans are included in the report.

We appreciate the cooperation and assistance we received from Business Affairs and University Technology Solutions throughout the review.

Respectfully,

John Lazarine, CIA, CISA, CRISC
Associate Vice President & Chief Audit Executive
Office of Internal Audit & Consulting Services

Distribution:

cc: Dr. Taylor Eighmy, President
Andrea Marks, Senior Executive Vice President, and Chief Operating Officer
Ginny Gomez-Leon, Senior Vice President and Chief Financial Officer
Sheri Hardison, Vice President for Financial Affairs and Chief Financial Officer
Michael Schnabel, Vice President and Chief Information Officer
Nassos Galiopoulos, Chief Technology Officer and Deputy Chief Information Officer
Fikret Sarisen, Chief Information Security Officer
Mary Hernandez, Senior Vice President for Administration and Operations
Stephanie Schoenborn, Chief of Police
Marco Garcia, Assistant Vice President of Supply Chain
Amy Tawney, Senior Vice President and Chief Human Resources Officer
Katy Madden, Vice President for People Excellence
J. Michael Peppers, Chief Audit Executive, UT System

External Audit Committee Members:
Randy Cain
Carol Severyn
Ed Garza
Albert Fernandez
Cari Takao
David Neuman
Eduardo Meza

OFFBOARDING AUDIT - ACADEMIC CAMPUS

INTERNAL AUDIT REPORT

February 3, 2026 | AUDIT REPORT # SAN25AS0005

Executive Summary

Background Information

Offboarding is a complex multistep process managed through HOP 4.14 Separation of Employment for UTSA Personnel, flowing from the separated employee's department to the following areas:

- People Excellence (Human Resources) – processes termination eForms in PeopleSoft
- University Technology Services (UTS) – updates Active Directory for the discontinuation or abridgement of network access
- Security Services – terminates physical access
- Payroll – determines final paycheck
- Inventory - ensures assets are returned and reassigned
- Credit Card (OneCard) Administration – ensures cards are canceled

Objective & Scope

For the FY25 Audit Plan, for the period of September 2024 through April 2025, assess the effectiveness of offboarding processes for separated employees to ensure:

- Network access (Active Directory, PeopleSoft, applications linked to Single Sign-On, etc.) was removed,
- Physical access (DSX card swipe) was removed,
- Separate employees were only paid for days worked,
- Tracked inventory was reassigned, and
- OneCards were disabled

Summary of Results and Conclusion

People Excellence, Payroll, and Credit Card offboarding functions operate effectively and in a timely manner. However, the following deficiencies were noted:

- Security Groups: Documentation and retention of allowable security groups for separated employees need enhancements. Employees with prior student status are addressed in the Privileged Accounts Internal Audit Report and not in this report.
- Physical Access: The automated process for disabling DSX swipe card access was not consistently effective.
- Asset Custody: Custodian records were not consistently updated to reflect the transfer of tracked assets from separated employees to the departments or to Surplus.

Additionally, oversight of the Separation Process may be beneficial in ensuring compliance with offboarding processes.

Summary of Findings

Internal Audit obtained management's action plans to address the findings identified during this audit. Those action plans and details of each finding are provided in each section of this report.

High	Former employees retain Active Directory Security Groups that are not documented or fully defined.	2/28/2026
Medium	Former employee accounts retained access to inappropriate security groups	7/31/2026
Medium	Former employees retain physical access.	3/31/2026
Medium	Inventoried assets are recorded in the custody of former employees.	3/31/2026
Medium	There is no assurance that departments complete the employee Separation Processing Checklist.	3/31/2026

See the Appendix for the finding rating definitions and methodology.

Detailed Audit Findings and Management Action Plans

HIGH

Finding #1: Former employees retain Active Directory Security Groups that are not documented or fully defined.

Condition:	Former employees are permitted to retain up to sixteen security groups within Active Directory. UTS does not have a current, authorized policy specifying which groups may be retained. Additionally, review of the Active Directory Administrative Center revealed that five of the sixteen groups lacked descriptions or documentation explaining their purpose.
Criteria:	OIS 1 Account Management: Owners of the data accessible through Active Directory must establish and document procedures for assigning, managing, and revoking access to all information under their control.
Cause:	The retention of security groups was informally approved and lacks formal documentation.

Impact: University staff are allowed to retain security groups with potential access to network resources. These groups cannot be readily determined as their descriptions and permissions are not defined.

Management's Action Plan:

1. There will be a review of the security groups and permission levels to determine the system resources the groups have access to.
2. There will be a review of the AD security groups designed to determine the appropriateness of each group and the level of permission rights assigned to the groups.
3. For the groups listed, management will perform an analysis.
   a) Retirees: Determine members within this group who only had access for 12 months from the date of retirement
   b) Legal Request: Ensure the group/or user requests are categorized in the system, and determine the appropriateness of the accounts with respect to the request documentation, which is set based on the duration (180 days) requested by Legal.
   c) Student (never expires): Determine if students are categorized in the same group for appropriateness. This will be addressed within eight weeks (i.e., by February 2026).
4. Evidence of the action plan, when executed, will be retained for internal audit to assess.

Responsible Parties:
Fikret Sarisen, Chief Information Security Officer
Nassos Galiopoulos, Chief Technology Officer and Deputy Chief Information Officer
Michael Schnabel, Vice President and Chief Information Officer

Planned Implementation Date:
February 28, 2026

Medium

Finding #2: Former employee accounts retained access to inappropriate security groups.

Condition:	Three former staff accounts retained credentials to inappropriate security groups post-termination. These security groups appear to provide capabilities such as: • Access to printer servers used by University Technology Services • Power User capabilities on local workstations • Access to Security Groups linked to the All-Faculty Staff Security Group
Criteria:	OIS 1 Account Management: Owners of the data accessible through Active Directory must establish and document procedures for assigning, managing, and revoking access to all information under their control.
Cause:	Active Directory does not track account changes, so it is unclear when or why these security groups were added, and the business reason for retaining them.

Impact: External parties with access to security group credentials can gain access to data retained in servers and devices such as:

- Retained print job data.
- Data saved to local workstations
- Data on servers and devices made available to Faculty and Staff.

Management's Action Plan:

- Phase 1: To be completed by February 2026 - Review and remove the three terminated accounts, if needed, from all inappropriate employee-related AD security groups, document before/after evidence, and update the provisioning process approved group list.
- Phase 2: To be completed by April 2026 - Develop and plan the release of an OIS 1–aligned access lifecycle procedure (group ownership, required justification/approval for privileged groups, and recurring access reviews/recertifications). Document business rules of engagement for account provisioning beyond the current process map.
- Phase 3 Audit & monitor: To be completed by July 2026 - Enable/centralize employee-related AD security group change auditing with alerts for sensitive group changes and for terminated/disabled accounts in privileged groups; provide quarterly compliance reporting to leadership.

Responsible Parties:
Nassos Galiopoulos, Chief Technology Officer and Deputy Chief Information Officer
Michael Schnabel, Vice President and Chief Information Officer

Planned Implementation Date:
July 31, 2026

Medium

Finding #3: Former employees retain physical access.

Condition:	Eight former employees did not have physical access removed from the DSX application due to holds or other conditions in Active Directory. The holds prevented automatic notification to Security Services to process the removal.
Criteria:	HOP 4.14 Separation of Employment for UTSA Personnel directs departments to notify Security Services to remove the departing employee's card access in the DSX application.
Cause:	Security Services receives Active Directory reports of employee separations when full deprovisioning criteria are met. Litigation or other holds prevent automatic deprovisioning. No evidence of communication from the eight employees' departments to Security Services for removal was found.

Impact: Former employees with active swipe card access may allow unauthorized entry to university facilities, assets, controlled materials, and personnel.

Management's Action Plan: The eight former employees identified in the audit no longer have physical access. Security Services removes physical access in DSX upon notification from either an automated Active Directory report or a direct notification from the department. The eight former employees identified were not communicated to Security Services through the standard means.

Security Systems has contacted UTS to request updates to the Active Directory export process to improve the accuracy and completeness of employee separation data, including:

- Adding Banner IDs.
- Addressing known issues that prevent automatic deprovisioning due to holds or other conditions.
- Expanding the daily extract to include additional fields related to terminations and transfers.

Discussions will be held with University Technology Support (UTS) to ensure terminated users with holds or exceptions unrelated to physical access are communicated for removal.

As described in the Management Action Plan for finding #5, discussions will be held with other leaders in this audit to identify potential process improvements to enhance offboarding oversight. Potential process improvements in the centralized and decentralized post-termination door access review to ensure the removal of physical access for former employees will be included in the discussions.

Responsible Parties:
Jessenia Skelton, Executive Director – Security Systems
Stephanie Schoenborn, Chief of Police
Mary Hernandez, Senior Vice President for Administration and Operations and Chief Operating Officer

Planned Implementation Date:
March 31, 2026

Medium

Finding #4: Inventoried assets are recorded in the custody of former employees.

Condition:	Eighteen assets were assigned to fourteen former employees. At least seven assets were not reassigned in the annual inventory process after the employees' departures.
Criteria:	HOP 4.14 Separation of Employment for UTSA Personnel directs departments to ensure all inventoried assets are collected. HOP 8.02 Property Accounting Responsibilities directs departments to communicate changes to the location or status of inventoried equipment and to perform the Annual Physical Inventory to account for inventoried assets.
Cause:	Departments are not timely in updating Asset Management records. The Inventory Department lacks an oversight mechanism to ensure that departments update inventory records in a timely and complete manner.

Impact: UTSA assets could be misappropriated or mislabeled, leading to improper recording and tracking of inventory possession.

Management's Action Plan: The Inventory Department notifies departments when personnel separate from the university and instructs them to reassign specified assets to current employees.

Ultimately, each department manager is responsible for maintaining their department's inventory records and ensuring accountability for all assigned assets.

As described in the Management Action Plan for finding #5, discussions will be held with other leaders in this audit to identify potential process improvements to enhance oversight of offboarding.

Potential process improvements in the assignment of inventoried assets for former employees will include:

- Establishing a formal follow-up timeline to monitor departmental responses and document instances of non-response upon receiving notification that an employee has separated from the university.
- Implementing a quarterly review process comparing separated personnel against assigned custodians.

Responsible Parties:
Blaine Walter, Senior Inventory Specialist
Javier Gonzales, Senior Manager Distribution Services
Marco Garcia, Assistant Vice President of Supply Chain
Sheri Hardison, Vice President of Financial Affairs and Chief Financial Officer

Planned Implementation Date: March 31, 2026

Medium

Finding #5: There is no assurance that departments complete the employee Separation Processing Checklist.

Condition:	The HOP 4.14 Separation Processing Checklist outlines the responsibilities of departments when employees are terminated. For example, the Checklist instructs departments to notify Security Services for the removal of physical access and to return property to the department's Inventory Contact Person. However, there is no assurance that the Checklist is completed by the department. • The Checklist is not required as part of the People Excellence Employee Separation Process. • The Checklist was last updated in March 2019. • The People Excellence Leadership Tool Kit Employee Separations is not included as a reference in HOP 4.14 and does not contain a functioning link to the Checklist.
Criteria:	The HOP 4.14 Separation of Employment for UTSA Personnel policy statement is to ensure consistent practices in terminating employment of UTSA personnel.
Cause:	HOP 4.14 does not outline an oversight mechanism to ensure the Separation Processing Checklist is completed and is provided to People Excellence as part of separation proceedings.

Impact: Separation processes may not be followed. For example, separated employees may retain physical access to university facilities and may retain university assets.

Management's Action Plan:

- The Separation Process Checklist was updated in 2023 and has now been updated in HOP 4.14.
- A link to the checklist was added to the Leadership Toolkit.
- The Leadership Toolkit is now included in the monthly HRBP email at least twice per year.
- People Excellence has scheduled a meeting with other leaders in this audit to brainstorm ways to ensure oversight in each area related to former employees.

Responsible Party: Katy Madden, Vice President for People Excellence

Planned Implementation Date: March 31, 2026

The following members of the Internal Audit & Consulting Service's staff performed the audit:
Aaron Sanders, Auditor III, CPA, CISA
Laura Buchhorn, Audit Director, CIA, CFE, CRMA, CCSA, CGAP

APPROVED FOR RELEASE

John Lazarine

John Lazarine, Chief Audit Executive, Internal Audit & Consulting Services

Distribution List

Copies of this report have been distributed to the following:

Taylor Eighmy PhD, President, UT San Antonio
Andrea Marks, Senior Executive Vice President, and Chief Operating Officer
Dr. Francisco Cigarroa, Senior Executive Vice President for Health Affairs and Health System
Ginny Gomez-Leon, Senior Vice President and Chief Financial Officer
Sheri Hardison, Vice President for Financial Affairs and Chief Financial Officer
Michael Schnabel, Vice President and Chief Information Officer
Nassos Galiopoulos, Chief Technology Officer and Deputy Chief Information Officer
Fikret Sarisen, Chief Information Security Officer
Mary Hernandez, Senior Vice President for Administration and Operations
Stephanie Schoenborn, Chief of Police
Marco Garcia, Assistant Vice President of Supply Chain
Amy Tawney, Senior Vice President and Chief Human Resources Officer
Katy Madden, Vice President for People Excellence

APPENDIX

Audit Methodology

We conducted this performance audit from April 18, 2025, through January 22, 2026, in accordance with the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. These standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Finding Rating Methodology and Definitions

Internal Audit used professional judgment to rate the findings identified in this report. The ratings identified for each finding were determined based on the degree of risk or effect of the findings with the audit objectives. In determining the ratings of audit findings, auditors considered factors such as the financial impact; potential failure to meet program/function objectives; noncompliance with state statute(s), rules, regulations, and other requirements or criteria; and the inadequacy of the design and/or operating effectiveness of internal controls. In addition, evidence of potential fraud, waste, or abuse; significant control environment issues; and little to no corrective action for issues previously identified could increase the ratings for audit findings. Internal Audit also identified and considered other factors when appropriate.

Priority	A finding identified by Internal Audit that may significantly affect a strategic or operational goal of a UT institution or the UT System if not addressed.
High	A finding identified by Internal Audit with a high risk of adverse effects to the UT institution or major units requires immediate management action to address the concern and mitigate organizational risks.
Medium	A finding identified by Internal Audit that carries a moderate likelihood of negative impact on the UT Institution—whether institution-wide or at the college, school, or unit level—requires management to implement corrective measures to address the concern and mitigate risks to an acceptable level.
Low	A finding identified by Internal Audit that is unlikely to negatively impact the UT Institution or any of its colleges, schools, or units. Management should still take steps to address the concern and lower risks for the organization.
Satisfactory	No reportable findings were identified during the audit.