Mobile Devices

Audit Report #20-103

August 26, 2020

The University of Texas at El Paso

Office of Auditing and Consulting

”Committed to Service, Independence and Quality”

The University of Texas at El Paso
Office of Auditing and Consulting Services

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

August 26, 2020

Dr. Heather Wilson
President, The University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Wilson:

The Office of Auditing and Consulting Services has completed a limited scope audit of Mobile Devices. During the audit, we identified opportunities for improvement and offered the corresponding recommendations in a separate management letter. We intend for the recommendations to assist in strengthening controls and help ensure the achievement of the University's mission, goals and objectives.

We appreciate the cooperation and assistance provided by the Information Security Office and Enterprise Computing staff during our audit.

Sincerely,

Lori Wertz

Lori Wertz
Chief Audit Executive

Report Distribution:

University of Texas at El Paso:
Ms. Andrea Cortinas, Vice President and Chief of Staff
Mr. Luis Hernandez, Vice President for Information Resources
Mr. Gerard Cochrane, Chief Information Security Officer
Ms. Guadalupe Valencia-Skanes, Associate Vice President for Business Affairs
Ms. Mary Solis, Director and Chief Compliance and Ethics Officer

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

Audit Committee Members:
Mr. Joe Saucedo
Mr. Fernando Ortega
Mr. Mark McGurk
Dr. John Wiebe
Dr. Giorgio Gotti
Mr. Daniel Garcia

Auditor Assigned to the Audit:
Victoria Morrison

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The Office of Auditing and Consulting Services has completed a limited scope audit of Mobile Devices to determine adherence to State and University security controls and standards. Due to the confidential nature of the audit, we issued a separate management letter to the Information Security Office, which details specific findings and recommendations. These confidential results are exempt from the Texas Public Information Act under Texas Government Code §552.139.

See “Audit Results” section for a table with the issues identified during the audit.

BACKGROUND

The Information Security Office (ISO) defines “mobile devices” as portable and self-powered devices, such as laptops, tablets, and smart phones. For purposes of this audit, we focused on University-owned and personal smart phones and tablets (hereinafter referred to as “mobile devices”).

According to the **Cisco Annual Internet Report (2018-2023),** there will be approximately 3.3 mobile devices/connections per person by 2023 in North America, up from 1.7 in 2018. With the flexibility provided by such devices and their availability, it is a balancing act for organizations to allow mobile devices to connect to its information resources, while still protecting those same information resources from the mobile devices.

At the University, mobile devices connect to University information resources (i.e. email services) via a tool called Microsoft Exchange ActiveSync, which allows users to synchronize their mobile devices to their University email. For the scope period of January 1, 2019 to June 2, 2020, there were approximately 6,000 connections to University information resources using mobile devices.

We performed this audit to assess the University’s mobile device policies/procedures, enforcement measures, and training/awareness activities.

AUDIT OBJECTIVES

Our objectives for the audit were to assess whether the University has a) policies and procedures in place to address mobile device security, b) methods to enforce these policies and manage such devices, and c) training and awareness of mobile device security.

SCOPE AND METHODOLOGY

The scope of the audit was limited to the period of January 1, 2019 to June 2, 2020.

We conducted the audit in accordance with the *International Standards for the Professional Practice of Internal Auditing* and the authoritative guidelines of the International Professional Practice Framework issued by the Institute of Internal Auditors.

The criteria and standards used were:

- Texas Administrative Code, Title 1, Part 10, Chapter 202, Subchapter C. §202.72 - Staff Responsibilities and §202.76 - Security Control Standards Catalog
- Texas Department of Information Resource-Security Control Standards Catalog Version 1.3 (TAC 202-76)
- UT System Policy (UTS 165) Information Resources Use and Security Policy and Standards
- UTEP ISO Information Resources Use and Security Policy and Standards

Our audit procedures included:

- interviewing and requesting information from key personnel,
- reviewing applicable laws, regulations, policies and procedures,
- verifying the existence of procedures and policies and awareness, and
- limited testing where appropriate

AUDIT RESULTS

Security Controls and Standards	Number of Findings
Enforcement of Mobile Device Policies	1
Review of Mobile Device Policies	1
Mobile Devices Training and Awareness	1

* Due to the confidential nature of the audit, we issued a separate management letter to the Information Security Office, which details specific findings and recommendations.

CONCLUSION

Based on the results of audit procedures performed, we conclude the ISO can strengthen existing security controls by implementing the recommendations included in the separate management letter, which contains confidential results exempt from the Texas Public Information Act under Texas Government Code §552.139.

We appreciate the cooperation and assistance provided by the Information Security Office and Enterprise Computing of Information and Resources and during our audit.