THE UNIVERSITY OF TEXAS AT DALLAS
OFFICE OF AUDIT AND CONSULTING SERVICES
800 W. CAMPBELL RD. SPN 32, RICHARDSON, TX 75080
PHONE 972-883-4876 FAX 972-883-6864

March 31, 2020

Dr. Richard Benson, President,
Ms. Lisa Choate, Chair of the Institutional Audit Committee:

We have completed an audit of mobile devices as part of our fiscal year 2019/2020 Audit Plans. The objective of our audit was to review the effectiveness of controls over mobile devices to ensure that UTD's data is adequately safeguarded. The report is attached for your review.

The audit resulted in opportunities to improve controls surrounding mobile device security and rates and plans. Management has reviewed the recommendations and has provided responses and anticipated implementation dates. Though management is responsible for implementing the course of action outlined in the response, we will follow up on the status of implementation subsequent to the anticipated implementation dates.

We appreciate the courtesies and considerations extended to us during our engagement. Please let me know if you have any questions or comments regarding this audit.

Toni Stephens, CPA, CIA, CRMA
Chief Audit Executive

Executive Summary

Audit Objective and Scope

The objective of our audit was to review the effectiveness of controls over mobile devices to ensure that UTD's data is adequately safeguarded. The scope of our audit was FY19.

Conclusion

Overall, the audit resulted in opportunities to improve controls surrounding mobile device security and rates and plans.

Audit Recommendations by Risk Level

Recommendation	Risk Level	Estimated Implementation Date
(1) *Develop Minimum Mobile Device Security Standards*	**Medium**	August 30, 2020
(2) *Develop a Process to Periodically Review Mobile Device Rates and Plans*	**Medium**	Completed

Responsible Vice Presidents

(1) Rafael Martin, Vice President and Chief of Staff
(2) Frank Feagans, VP and Chief Information Officer

Responsible Parties

(1) Nate Howe, Chief Information Security Officer
(2) Brian Dourty, Associate VP for Information Technology and Chief Technology Officer
- John Patterson, Director of Information Technology – Networking
- Korky Kathman, IT Support Specialist II

Staff Assigned to Audit

Project Leader: Rene Herrera, CISA, CFE, IT Audit Manager
Staff: Chris Robinette, Auditor II; Siddharth Joshi and Amruta Mujumdar, Student Interns

Report Distribution

Members of the UT Dallas Institutional Audit Committee
External Members
- Ms. Lisa Choate, Chair
- Mr. Gurshaman Baweja
- Mr. John Cullins
- Mr. Bill Keffler
- Ms. Julie Knecht

UT Dallas Members
- Dr. Richard Benson, President
- Mr. Rafael Martin, Vice President and Chief of Staff
- Dr. Kyle Edgington, Vice President for Development and Alumni Relations
- Mr. Frank Feagans, Vice President and Chief Information Officer
- Dr. Gene Fitch, Vice President for Student Affairs
- Dr. Calvin Jamison, Vice President for Facilities and Economic Development
- Dr. Inga Musselman, Provost and Vice President for Academic Affairs
- Ms. Sanaz Okhovat, Chief Compliance Officer
- Dr. Joseph Pancrazio, Vice President for Research
- Mr. Terry Pankratz, Vice President for Budget and Finance
- Mr. Timothy Shaw, University Attorney, ex-officio

UT Dallas
- Responsible Parties listed above
- Mr. Bob Fishbein, Associate VP for Auxiliary Services
- Peggy Attari, Associate Director, Office of Information Technology

External Agencies
The University of Texas System
- System Audit Office

State of Texas Agencies
- Legislative Budget Board
- Governor's Office
- State Auditor's Office

Table of Contents

Background

Mobile devices at UT Dallas are defined as "*Laptops, tablets, smart phones, or other devices designed to be easily portable that are capable of creating, storing, or processing University Data*.[1]" The majority of mobile devices are personally owned and not directly managed by IT staff, though the Information Security Office defines risk-mitigating connection requirements implemented by the Office of Information Technology. In the past year, approximately 4,300 mobile devices established over 11,000 unique connections to UTD email servers from various email applications. The offices responsible for handling mobile devices include:

Information Security Office (ISO): Security policies and procedures and related controls for connections to the UTD network are under the responsibility of the Information Security Office, reporting to the Vice President and Chief of Staff. The Information Security and Acceptable Use Policy (UTDBP3096) establishes security requirements and privacy expectations for University-owned mobile devices.

Office of Information Technology (OIT): The OIT Telecommunications Group, within the Systems, Security, and IT Architecture department, supports University-owned devices and data plans and also works with the mobile service vendors to determine the best phones and services to meet the University's needs. The Cellular Communications Equipment Policy (UTDBP3008) provides guidance regarding the acquisition and use of cellular communications equipment and associated services for University business use.

Inventory: Inventory reports to Auxiliary Services under the leadership of the VP for Facilities and Economic Development. They are responsible for and managing the property tagging and tracking process for University-owned mobile devices as outlined at UTDBP3066, *Property Administration*.

Cost Savings

Prior to the audit, the University provided cellular allowances and equipment to supplement the costs of using personal devices for incidental use for employees who would frequently engage in work-related travel, were "on call" for essential services, and/or were members of key personnel needed in an event of an emergency.

Expenses for such allowances were approximately $1 million for about 504 users from FY18-19.

During the audit, discussions were held with management regarding the costs to administer the program.

In September 2019, the cellular allowances were discontinued, resulting in future cost savings to the University.

Tracking Mobile Devices

Property purchased by UTD is required to be tagged and tracked in accordance with UTD policies, outlined at UTDBP3066, *Property Administration*. Without controls over tagging and tracking mobile devices, inventory may be misstated and the risk of mobile devices being lost and/or stolen is increased.

Audit and Consulting Services recommended during the audit that Inventory should develop a process to tag and track University-purchased mobile phones in the property inventory system. As a result, a process was developed by Inventory, and mobile phones have been tagged and tracked since April 2019.

[1] https://policy.utdallas.edu/utdbp3096

Audit Objective

The objective of our audit was to review the effectiveness of controls over mobile devices to ensure that UTD's data is adequately safeguarded.

Scope and Methodology

The scope of this audit was FY19. Exit conferences were held with management and responsible parties in August 2019; however, the report was not completed until March 2020, due to limited resources and various discussions necessary to fully understand management's risk mitigating plans.

To satisfy our objectives, we performed procedures that included the following:

- Interviewing responsible parties from the various departments responsible for mobile devices.
- Reviewing OIT and ISO policies and procedures in place to grant and secure connections to UTD data from mobile devices, including the cellular allowance policy, mobile device and service plan procedures, and the NetID Plus (DUO) security application process.
- Reviewing the security vulnerabilities and patch levels of devices connecting to the network with Microsoft EAS (Exchange ActiveSync).

We conducted our examination in conformance with the guidelines set forth in The Institute of Internal Auditor's *International Standards for the Professional Practice of Internal Auditing*. The *Standards* are statements of core requirements for the professional practice of internal auditing.

Additionally, we conducted the audit in accordance with generally accepted government auditing standards, as applicable. Those 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Audit Results and Management's Responses

Strengths and Controls Noted During the Audit
ISO uses a two-factor authentication application to increase account/data security.
OIT has formal procedures in place for the purchase and management of mobile phone and data plans purchases.

Although the above strengths and controls were noted, other opportunities to strengthen controls over mobile devices are listed below. Risk levels are defined in the appendix on page 9.

Observation	Risk/Effect	Recommendations and Management's Responses
(1) ***Develop Minimum Mobile Device Security Standards*** The Information Security Office is responsible for determining the security policies and procedures for devices connecting to the UTD data/network in coordination with related areas such as the Office of Information Technology. Staff, faculty, and students primarily connect to UTD data such as email using a mobile device or mobile email application such as Microsoft Outlook. Mobile devices on the wireless network can attempt connections to resources on the wired network and therefore pose risk to UTD assets if compromised. the Information Security Office has excluded devices on the wireless network from routine vulnerability scanning due to transient usage patterns and the majority of devices being personally owned and not managed by UTD. The ISO Office has additional controls in place to secure connections from mobile devices to the UTD network using the NetID Plus DUO application. The DUO security application will alert the user anytime their UTD NetID account is being used to authenticate and the user can deny the connection if the login attempt is not them. The NetID Plus/DUO application can also be used to restrict access and authentication from certain operating systems and applications if using outdated software. However, the NetID Plus/DUO application is not configured to restrict access and authentication from mobile devices running outdated software or devices that have been tampered with (jailbroken). At this time, mobile phones connecting to the UTD network are not required to run a UTD approved operating system (OS) or mail	**Medium** Without an established minimum standard mobile device operating system (OS), devices may be running out-of-date software with active security vulnerabilities. In addition, without mobile device vulnerability scanning, devices may be running in a "tampered" (jailbroken) mode and be running unauthorized software and applications that pose a security threat to the wired network.	**Recommendation:** ISO should develop minimum mobile device operating system and application configuration standards for devices connecting to UTD resources. In addition, consider the use of NetID Plus (DUO) for mobile device protections. **Management's Response and Action Plan:** The ISO will document minimum allowed software versions within our Standard for Mobile Computing Devices. We will then identify methods to measure compliance, notify users of non-compliance, and disallow devices when outdated software poses a risk to UTD assets. Additionally, our Duo roadmap will be updated to consider applicability for protecting mobile devices. **Estimated Date of Implementation:** 8/30/2020 **Person Responsible for Implementation:** Nate Howe, Chief Information Security Office (CISO) for UT Dallas

Observation	Risk/Effect	Recommendations and Management's Responses
applications to ensure they meet minimum UTD security standards. At the time of the audit, there were approximately 11,185 active connections to the email server, of which 4,389 were from mobile devices (Apple iOS and Android) and 6,796 were from Outlook email applications. Specifically, 350 (10 percent) of Apple devices and 54 (six percent) of Android devices were running outdated software with active vulnerabilities.		
(2) ***Develop a Process to Periodically Review Mobile Device Rates and Plans*** UTD funded over 100 phone/data plan lines with approximately $4,129 in monthly recurring costs (MRCs) and overages which totaled about $65,000 in annual expenses. The lines had not been reviewed periodically, and UTD was operating under outdated Texas Department of Information Resources (DIR)s rates which were over two years old. During the audit, Telecommunications and Internal Audit reviewed the phone/data plans process for potential cost savings that resulted in annual MRC savings of about 14% ($9,100): • Telecommunications updated the plans to the current DIR-approved rates which resulted in savings of $4,770 in MRC savings. • In addition, an audit review of the active Telecommunications lines resulted in the cancellation of eight lines that were no longer in use which resulted savings of $4,330 MRC savings.	**Medium** Without a process to review mobile phone/data plans periodically, UTD may be offering plans that do not meet the business needs and may be paying higher rates than necessary.	**Recommendation:** The Telecommunications group should develop a process to periodically review mobile device rates and plans to ensure UTD is contracting with the plans that meet the business needs of UTD and are approved by DIR. **Management's Response and Action Plan:** DIR contracts are negotiated by the carriers on a periodic basis. Once negotiated, the carrier representative reaches out to UTD procurement for a letter to update the new DIR pricing for all of our accounts. The most recent occurrence started in April of 2019 and concluded in May 2019 with a signed DIR Contract, so we are up to date. Incremental changes are automatically applied to our account (i.e. new equipment, etc.). This process is outside of UT Dallas control. The University of Texas at Dallas issued cellular devices are managed under a contracted rate from The Department of Information Resources. The DIR pricing does not change very often and when it does these rates are automatically applied to our contracts. The Office of Information Technology will continue to follow up with the carriers annually to see if there are changes to any of the plans or other carrier options that would benefit the University. These

Observation	Risk/Effect	Recommendations and Management's Responses
		changes would mainly include specific promotions that we would leverage where applicable. There are some legacy plans that users are on that for various reasons, mainly pricing. OIT will continue to monitor these contracts to make sure they are still the best contract for the users. An annual process has been implemented to request departments to review and confirm Telecom cellular/data devices are still in use and needed. We have recently seen the plan for an adoption of a new cellular equipment policy that significantly dictates the use of university-owned devices. We have instituted a procedure whereby this policy is sent to anyone that is submitting a request for cellular device service, informing them that any TSR submitted with an authorized signature acknowledges compliance with the new policy. **Estimated Date of Implementation:** Completed **Person Responsible for Implementation:** • Brian Dourty, Associate VP and Chief Technology Officer • John Patterson, Director of Information Technology – Networking • Korky Kathman, IT Support Specialist II

Conclusion

Based on the audit work performed, we conclude that there are opportunities to improve controls surrounding mobile device security and rates and plans.

We appreciate the courtesy and cooperation received from the management and staff in the Offices of Information Security, Information Technology, Inventory, and Budget and Finance as part of this audit.

Appendix

Definition of Risks

Risk Level	Definition
Priority	High probability of occurrence that would significantly impact UT System and/or UT Dallas. Reported to UT System Audit, Compliance, and Risk Management Committee (ACRMC). Priority findings reported to the ACRMC are defined as "*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	Risks are considered to be substantially undesirable and pose a moderate to significant level of exposure to UT Dallas operations. Without appropriate controls, the risk will happen on a consistent basis.
Medium	The risks are considered to be undesirable and could moderately expose UT Dallas. Without appropriate controls, the risk will occur some of the time.
Low	Low probability of various risk factors occurring. Even with no controls, the exposure to UT Dallas will be minimal.