The University of Texas at Tyler

Information Technology Inventory and Laptop Encryption Audit Report

August 2013

THE UNIVERSITY OF TEXAS AT TYLER AUDIT OFFICE
3900 UNIVERSITY BLVD.
TYLER, TEXAS 75703

The University of Texas at Tyler
Information Technology Inventory and Laptop Encryption Audit
Fiscal Year 2013

Executive Summary

In the spring of 2012, The University of Texas (UT) System experienced a significant breach of confidential information at one of our institutions. In June 2012, The UT System Executive Vice Chancellor (EVC) for Academic Affairs and the EVC for the Health Affairs sent an official laptop encryption memorandum to their respective UT academic and health institution presidents which required that all University laptops and personally-owned computers used to conduct any University business be encrypted by August 31, 2012.

At the request of executive management and the UT System Board of Regents, audits of both the information technology (IT) inventory process and the laptop encryption are being performed at all the institutions during the current fiscal year. As a result of the request, the audit was added to the University of Texas at Tyler's Fiscal Year 2013 Audit Plan. To ensure consistent audit objectives are achieved, the UT System Audit Office created and communicated audit guidance to all UT institutions.

From the procedures performed, we did not identify any findings or have any recommendations.

Background

In June 2007, the System-wide Chief Information Security Officer issued a security bulletin which established encryption requirement practices for portable and non-portable University-owned computing devices that contain confidential data. In June 2012, the EVC for Academic Affairs and the EVC for Health Affairs sent an official laptop encryption memorandum to each UT academic and health institution's president.

The memorandum established deliverables and deadlines, which included:

- Setting a deadline for the encryption of all institutional laptop computers and personal computers used to conduct any University business; [1]
- Requiring each institution to encrypt 100 percent of laptop computers by August 31, 2012; and
- Requiring institutions to report to their EVC and to the UT System Chief Information Security Officer;
    - The number of laptops owned by the institution as of August 31, 2012;
    - The number of laptops encrypted as of August 31, 2012;
    - The rate at which laptop computers were being encrypted; and
    - The institutional plan to achieve 100 percent encryption compliance.

Historically, institutions have been required to track assets in accordance with the Texas Comptroller of Public Accounts' State Property Accounting System (SPA). SPA requires all hand guns and rifles, as well as all controlled property over $500 to be recorded and reported. Although the encryption memorandum does not specifically state that the institution's laptops need to be recorded within an asset management system, it does require and institution to have an accurate count of laptops and that they are encrypted or exempted.

[1] On May 1, 2013, the UT System Office of Academic Affairs issued a memorandum removing the requirement to encrypt personal computers unless they contained confidential data.

The University of Texas at Tyler
Information Technology Inventory and Laptop Encryption Audit
Fiscal Year 2013

Engagement Objectives

The objectives of this audit were to:

- Gain an understanding of the key internal controls over the IT asset management process at UT Tyler;
- Determine whether the key controls are adequate to track and record IT inventory;
- Determine whether UT Tyler's laptop inventory is complete, accurate, and up-to-date; and
- Determine whether all UT Tyler laptops and personal computers that contain confidential data and are used for University business have been properly encrypted or exempted.

Scope and Methodology

The scope of this audit encompassed all UT Tyler IT inventory and policies related to personally owned computers used to conduct university business that contain confidential data.

Standards

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

Procedures

To accomplish the objectives of this audit, we:

- Reviewed UT Tyler's internal policies;
- Reviewed questionnaires completed by UT Tyler personnel;
- Conducted interviews with central receiving, IT personnel and departmental personnel;
- Selected a sample of assets from the DEFINE accounting system purchasing records between September 1, 2012 and April 25, 2013 to determine whether they were appropriately recorded in the DEFINE inventory records;
- Selected a sample of laptops from DEFINE inventory records to determine whether they a were appropriately tagged, available for inspection, and were encrypted or appropriately exempted;
- Selected a sample of laptops throughout campus to determine whether they were appropriately tagged, available for inspection, recorded within UT Tyler's inventory records, and were encrypted or appropriately exempted; and
- Verified UT Tyler has a policy that states "any Confidential University Data stored on a Portable Computing Device or Non-University Owned Computing Device must be encrypted..." however, testing of non-university owned computers for confidential data and encryption was not included in this audit.

Engagement Results

According to The University of Texas System, a significant finding is one that may be material to the operation, financial reporting, or legal compliance of the university if corrective action has not been fully implemented. This would include an internal control weakness that does not reduce the risk of irregularities, illegal acts, errors, inefficiencies, waste, ineffectiveness, or conflicts of interest to a reasonably low level.

This audit resulted in no recommendations to UT Tyler operations. As a result of our testing we found IT purchases are properly recorded in DEFINE, laptop inventory is complete, accurate and current, all laptops are properly encrypted or appropriately exempted, and UT Tyler policy requires all devices including Non-University Owned Computing Device that store confidential University Data must be encrypted.

Conclusion

UT Tyler's key controls over IT inventory and laptop encryption appear to be adequate to properly record IT inventory and assure laptops are encrypted or exempted as required. Additionally, UT Tyler policy requires all devices including Non-University Owned Computing Device that store confidential University Data must be encrypted. We appreciate the assistance of Financial Services and IT Security personnel during this engagement and commend the departments on their compliance with university requirements.

Lou Ann Viergever

Lou Ann Viergever, CPA, CIA, CRMA
Executive Director of Audit and Consulting Services