December 20, 2013

Dr. Daniel,

We have completed an audit of Laptop Encryption as part of our fiscal year 2013 Audit Plan, as required by UT System and the report is attached for your review. The audit was conducted in accordance with the Institute of Internal Auditors’ International Standards for the Professional Practice of Internal Auditing. The objectives of the audit were to:

- determine whether laptop inventory, for University owned and personal laptops used to conduct University business, is complete, accurate, and up-to-date;
- determine whether all laptops have been properly encrypted or exempted; and
- gain an understanding of key internal controls over the information technology (IT) asset management process to determine whether they are adequate to track and record IT inventory.

Overall, we found that improvements are necessary in order to ensure that laptops encryption requirements have been adequately met. The attached report details recommendations that will help enhance controls over encryption requirements and documentation.

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
Executive Director of Audit and Compliance

UT Dallas Responsible Parties:
Dr. Sue Taylor, Acting Chief Information Security Officer

Members of the UT Dallas Audit and Compliance Committee:
Dr. Hobson Wildenthal, Executive Vice President and Provost
Dr. Calvin Jamison, Vice President for Administration
Mr. Terry Pankratz, Vice President for Budget and Finance
Dr. Andrew Blanchard, Vice President for Information Resources and Chief Information Officer
Dr. Bruce Gnade, Vice President for Research
Dr. Darrelene Rachavong, Vice President for Student Affairs
Dr. James Marquart, Vice Provost
Dr. Sue Taylor, Acting Chief Information Security Officer
Mr. Timothy Shaw, University Attorney
Ms. Lisa Choate, Partner, Ultimate Health Resources

The University of Texas System:
Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs
Alan Marks, Attorney
Mr. J. Michael Peppers, CIA, CRMA, CPA, FACHE, Chief Audit Executive
Ms. Moshmee Kalamkar, CPA, CIA, Audit Manager

State of Texas Agencies:
Legislative Budget Board
Governor’s Office
State Auditor’s Office
Sunset Advisory Commission

AN EQUAL OPPORTUNITY/AFFIRMATIVE ACTION UNIVERSITY
Executive Summary

_Laptop Encryption Audit, Report No. 1406_

**Audit Objective and Scope:** The audit objectives were to: determine whether laptop inventory, for University owned and personal laptops used to conduct University business, is complete, accurate, and up-to-date; determine whether all laptops have been properly encrypted or exempted; and gain an understanding of key internal controls over the information technology (IT) asset management process to determine whether they are adequate to track and record IT inventory. The scope of the audit was fiscal year 2013 operations.

**Audit Results:**
The audit resulted in no recommendations considered significant to university operations. However, we offer the following recommendations to ensure the university can achieve compliance with encryption requirements.

<table>
<thead>
<tr>
<th>Recommendation</th>
<th>Estimated Implementation Date</th>
</tr>
</thead>
<tbody>
<tr>
<td>(1) Enhance Inventory Controls</td>
<td>June 30, 2014</td>
</tr>
<tr>
<td>(2) Develop Policy for Naming of Assets</td>
<td>June 30, 2014</td>
</tr>
<tr>
<td>(4) Improve Documentation for Exemption Approvals</td>
<td>June 30, 2014</td>
</tr>
</tbody>
</table>

**Conclusion:** Overall, the Information Security Office appears to have made significant progress in encrypting laptop devices. However, certain improvements are required. Implementation of the recommendations outlined in this report will further enhance internal controls and compliance with UT System policies, and best practices.

**Responsible Vice President:**
Mr. Terry Pankratz, Vice President for Budget and Finance

**Responsible Party:**
Dr. Sue Taylor, Interim CISO

**Staff Assigned to Audit:**
Ali Subhani, CIA,CISA,GSNA, IT Audit Manager
Table of Contents

Background ................................................................................................................................. 4

Audit Objectives ....................................................................................................................... 5

Scope and Methodology ........................................................................................................... 5

Audit Results and Management’s Responses ........................................................................... 5

Audit Recommendations .......................................................................................................... 6
  (1) Enhance Inventory Controls ......................................................................................... 6
  (2) Develop Policy for Naming of Assets ........................................................................... 7
  (3) Enhance Encryption Practices on Computing Devices Not Owned by the University ........................................................... 7
  (4) Improve Documentation for Exemption Approvals ...................................................... 8

Conclusion ................................................................................................................................. 9
Background

In 2007, The University of Texas System (Administration) issued a bulletin, “Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices (SPB-1)\(^1\),” which lays out the basic expectations and requirements for the encryption of laptop computers at UT System. However, in 2007 no single solution was available to encrypt all laptop platforms, and many institutions did not readily adopt a solution. Since 2007, UT System has experienced several incidents of lost or stolen laptops containing confidential or sensitive data. As a result, the Executive Vice Chancellors in Health Affairs and Academic Affairs issued a memo to each institutional president which required all institutions to report their current state of laptop encryption and their plan to encrypt all laptops. The memo required each institution to report this information by July 1, 2012. In addition, UT System requested that audits of all institutions be performed to assess the status of encryption.

At UT Dallas, the project for encrypting laptops was spearheaded by the Information Security Office (ISO). The department hired additional contractors and employees which supported the Information Security staff to help encrypt laptops around campus. According to Information Security's metrics, there are a total of 2,760 laptops on the University’s property inventory records. As of July 31 2013, a total of 2,275 laptops had been encrypted, 266 remain unencrypted, 197 were identified as missing, and 21 were in the process of being sent to surplus since the devices could not handle encryption software.

\[\text{Laptop Encryption Status}\]

*As of July 31, 2013*

\[\text{http://www.utsystem.edu/ciso/SPB1-FAQ.pdf}\]
Audit Objectives

The audit objectives were to:

1. determine whether laptop inventory, for University owned and personal laptops used to conduct University business, is complete, accurate, and up-to-date;
2. determine whether all laptops have been properly encrypted or exempted; and
3. gain an understanding of key internal controls over the information technology (IT) asset management process to determine whether they are adequate to track and record IT inventory.

Scope and Methodology

The scope of this audit was FY 2013 operations. Our fieldwork concluded on November 5, 2013. To satisfy our objectives, we performed the following:

- Gained an understanding of laptop encryption requirements.
  - Examined the Executive Vice Chancellor’s Encryption Memo and FAQ’s.
  - Examined the system-wide encryption bulletin. ([http://utsystem.edu/ciso/spb1.pdf](http://utsystem.edu/ciso/spb1.pdf))
  - Obtain and reviewed the University’s encryption plan

- Gained an understanding of the laptop inventory and encryption process.

- Identified controls that ensure that the laptop inventory is accurate, complete, and up to date.

Where applicable, we conducted our examination in accordance with the guidelines set forth in The Institute of Internal Auditor’s *International Standards for the Professional Practice of Internal Auditing*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance or audit work, and management of the internal auditing department.

Audit Results and Management’s Responses

Overall, it appears that UT Dallas has not fully complied with the encryption requirements that were mandated by UT System. Our audit work indicated that the following controls currently exist:

- The ISO has been provided the necessary tools and personnel to encrypt the laptops.
- The ISO has prepared a plan on how the institution will implement encryption capability across campus.
A significant recommendation is defined as one that may be material to operations, financial reporting, or legal compliance. 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 reasonable low level. We have no significant recommendations resulting from this audit; however, the following recommendations will help enhance compliance with UT System requirements.

**Audit Recommendations**

(1) **Enhance Inventory Controls**

According to UTD property inventory policies, “IPAD’s, laptops, and desktop computers, are to be added to inventory records regardless of the dollar value.” During the audit process, we identified 10 assets (two laptops, one netbook and seven tablets) that were not added to the official property inventory records, because these assets were purchased using university-issued purchasing cards. University policies prohibit the purchase of such items using a purchasing card. Without a complete inventory, the ISO cannot ensure that the assets get encrypted.

Additionally, during analysis of networking records that indicated the electronic names of computing devices that had connected to the UTD network, we noted 168 computing devices that were not on official property inventory records. The devices appeared to be laptops based on the way they were named. However, due to a lack of relevant logs and infrastructure, we could not determine if the devices met the criteria for encryption and the time when the devices last connected to the UTD network. According to TAC 202.75, “Information resources systems shall provide the means whereby authorized personnel have the ability to audit and establish individual accountability for any action that can potentially cause access to, generation of, modification of, or effect the release of confidential information.”

**Recommendation:** The process for ensuring all information technology assets are added to property inventory regardless of the dollar value should be improved. Additionally, processes should be enhanced to ensure that computing devices that have connected to the UTD network are being appropriately encrypted if they meet the relevant criteria for encryption.

---

2 [http://www.utdallas.edu/audit-compliance/training/PropertyInventory.pdf](http://www.utdallas.edu/audit-compliance/training/PropertyInventory.pdf)

Management’s Response: The Office of Information Security will work collaboratively with the Office of Property Administration and Information Resources to identify methods to improve and validate the capture of critical information about technology assets that will provide assurance that devices are in compliance with encryption policy.

Estimated Date of Implementation: June 30, 2014

Person Responsible for Implementation: Director, Logistics and Distribution; IR-AVP Operations; CISO

(2) Develop Policy for Naming of Assets

The responsibility for maintaining property inventory records resides with the Office of Inventory and Surplus Control; whereas, the responsibility for having an up-to-date listing of electronic assets currently rests with the ISO. There is currently no policy that mandates that the electronic name of an asset should match the property tag that has been assigned to the device. As a result, the ISO is burdened by having to rely on a complex reconciliation process when reconciling property inventory records to reports that are generated from security tools. According to best practices, it is prudent to have procedures in place that will allow for more efficient reconciliations.

Recommendation: Procedures should be developed in Information Security that require the electronic name of computing devices to match up to the assigned property tag.

Management’s Response: The Office of Information Security will work collaboratively with the Office of Property Administration and Information Resources to develop an enhanced naming convention that will clearly identify desktops, laptops and mobile devices.

Estimated Date of Implementation: June 30, 2014

Person Responsible for Implementation: Director, Logistics and Distribution, Director of Purchasing, CISO

(3) Enhance Encryption Practices on Computing Devices Not Owned by the University

According to Security Practice Bulletin (SBP) # 1, encryption was established as a requirement for non-university owned computing devices. In order to comply with UT System encryption requirements, the ISO sent out a survey in October 2012 that

4 http://utsystem.edu/ciso/SPB1.pdf
required university employees to voluntarily communicate whether non-university owned computing devices were being utilized for storage of confidential data. The ISO only received responses from 1,152 employees, representing about 22% of total employees. Due to the low response rate and not having further attempts to communicate with the remaining employees, UT Dallas cannot demonstrate full compliance with UT System requirements, and the potential for unencrypted data being stored on non-university owned computing devices is increased.

**Recommendation:** The ISO should put a process in place to ensure that all university employees formally acknowledge that confidential data on non-university owned computing devices is appropriately protected.

**Management’s Response:** According to the document ‘Operating Standards for Non-University Owned Computers’ dated October 18, 2012, the owner of said system(s) must escrow the cryptographic key with the Office of Information Security and sign a statement indicating their computer is encrypted and state the encryption method used. This acknowledgment must be renewed annually. The ISO has recently implemented a process whereby users will be notified via email to revalidate their computer usage a month in advance of their yearly anniversary.

**Estimated Date of Implementation:** June 30, 2014

(4) **Improve Documentation for Exemption Approvals**

The encryption requirements from UT System allowed for exemptions to the use of encryption on computing devices under certain circumstances. However, according to SBP # 1,\(^5\) “exceptions must be documented.” Additionally, guidance from UT System required that exceptions be approved by the UT System CISO. During the audit, the ISO was unable to provide documentation detailing the assets that were granted exemptions from encryption requirements. Many of the exemptions were maintained in the CISO’s inbox; however, many others could not be located. Therefore, we were unable to verify whether the exemptions were appropriately authorized and in line with UT System requirements.

**Recommendation:** The CISO should develop improved record-keeping for any devices that are granted exemptions from encryption requirements. These exemptions should be retained in a central location and not within an employee’s email inbox.

**Management’s Response:** The Office of Information Security will request that an OnBase repository be created for the storage of the scanned encryption exemption forms along with a database repository to track individual forms. Reports will be emailed to the Deans and administrative management for annual review and validation.

\(^5\) [http://utsystem.edu/ciso/SPB1.pdf](http://utsystem.edu/ciso/SPB1.pdf)
Estimated Date of Implementation: June 30, 2014

Person Responsible for Implementation: CISO, EAS-OnBase technical support team

Conclusion

Based on the audit work performed, we conclude that overall, the Information Security Office appears to have made significant progress in encrypting laptop devices. However, certain improvements are required. Implementation of the recommendations outlined in this report will further enhance internal controls and compliance with UT System policies, and best practices.

We appreciate the courtesy and cooperation received from the management and staff of Information Security Office and Information Resources during this audit.