The University of Texas at Brownsville

FY 2013 Audit of Laptops Encryption

May 29, 2013

OFFICE OF INTERNAL AUDITS

The University of Texas at Brownsville

Norma L. Ramos, CIA, CGAP

Director of Internal Audits

May 29, 2013

Dr. Juliet V. Garcia, President
The University of Texas at Brownsville
80 Fort Brown
Brownsville, Texas 78520

Dear Dr. Garcia:

As part of our Audit Plan for fiscal year FY 2013, we completed the **FY 2013 Audit of Laptops Encryption** at The University of Texas at Brownsville. The objectives of this audit were:

- Determine whether laptop inventory at UT Brownsville is complete, accurate, and up-to-date; and
- Determine whether all institutional laptops have been properly encrypted or exempted.

Our examination was conducted in accordance with guidelines set forth in The University of Texas System's Policies UTS 129 and the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing (Standards)*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance of audit work, and management of internal auditing department. UTS 129 requires that we adhere to the *Standards.*

The recommendations in this report represent, in our judgment, those most likely to provide a greater likelihood that management's objectives are achieved. The recommendations differ in such aspects as difficulty of implementation, urgency, visibility of benefits, and required investments in facilities and equipment, or additional personnel. The varying nature of the recommendations, their implementation costs, and their potential impact on operations should be considered in reaching your decision regarding courses of action.

We appreciate the assistance provided by UTB's management and other personnel. We hope the information and analyses presented in our report are helpful.

Sincerely,

Norma L. Ramos

Norma L. Ramos, CIA, CGAP
Director of Internal Audits

cc: *The University of Texas at Brownsville*
Dr. Alan F. J. Artibise, Provost and Vice President for Academic Affairs
Ms. Rosemary Martinez, CPA, Vice President for Business Affairs
Dr. Hilda Silva, Vice President for Student Affairs
Dr. Silva Leal, Vice President for Enrollment Management
Mr. Irvine W. Downing, Vice President for Institutional Advancement and
Vice President for Economic Development and Community Services
Dr. Luis Colom, Vice President for Research
Dr. Clair Goldsmith, Vice President for Information Technology Services and Chief Information Officer
Dr. Marilyn Woods, Executive Assistant to the President

UT System Administration
Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs, *Ad Interim*
Mr. Michael Peppers, Chief Audit Executive, UT System Audit Office
Ms. Paige Buechley, Assistant Director, UT System Audit Office

Table of Contents

Executive Summary

The FY 2013 approved audit plan included the FY 2013 Audit of Laptops Encryption. 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 (EVC's) 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 objectives of the audit were to:

- Determine whether laptop inventory at UT Brownsville is complete, accurate, and up-to-date; and
- Determine whether all institutional laptops have been properly encrypted or exempted.

We made observations and recommendations over the following areas:

- Discrepancies between Accounting and Finance Inventory List and User Support Services-ITS SharePoint lists
- Laptops not encrypted
- Violation of Security Procedures Bulletin 1- "using products and/or methods approved by the Entity's Chief Information Security Officer"
- Refusal of encryption mandate by user

We concluded that the laptop inventory at UT Brownsville is not complete, accurate, and up-to-date due to the discrepancies between the Accounting and Finance Inventory List and the ITS Sharepoint List. In addition, not all institutional laptops have been properly encrypted or exempted in accordance with the UT System Encryption requirement. Failure to properly encrypt laptops could expose sensitive University data and could lead to costly remediation efforts and negative publicity.

Background Information

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),” 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 (EVC’s) 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.

For FY 2013, the System Audit office asked each institution to include audit plan hours to report on the status of encryption at their institution.

Audit Objectives

The objectives of the audit were to:

- Determine whether laptop inventory at your UT Brownsville is complete, accurate, and up-to-date; and
- Determine whether all institutional laptops have been properly encrypted or exempted.

Scope of Work

All institutional laptop computers (including personal computers that faculty or staff may use to conduct **any** university business), and policies and procedures related to laptop encryption process at UTB. We did not include any desktop computers in our scope.

Our examination was conducted in accordance with guidelines set forth in The University of Texas System’s Policies UTS 129 and the Institute of Internal Auditors’ *International Standards for the Professional Practice of Internal Auditing (Standards)*. The *Standards* set criteria for internal audit departments in the areas of independence, professional proficiency, scope and performance of audit work, and management of internal auditing department. UTS 129 requires that we adhere to the *Standards.*

Audit Results

The Office of Information Security is responsible for coordinating and verifying the encryption of laptops at the University of Texas at Brownsville. The User Support Services (USS) of the Information Technology Services Division (ITS) is responsible for the actual encryption of university laptops. The process consists of ITS sending communications and collecting laptops from departments, encrypting and logging encryption status, and finally returning laptop to the departments. A SharePoint site is maintained by User Support Services (USS - ITS Division) where all laptops encrypted or pending encryption are logged. In addition, the console (Secure Doc, Safeboot) shows the encryption status for laptops and the last time the laptop logged into the network. Accounting and Finance also maintains an inventory list of assets. Laptops are added to this list when they are purchased.

In addition ITS, Standard Operating Procedure SOP 1.1.1 will be updated to include the new process to order laptops and ensure encryption software is installed before delivering the laptop to end user.

Inventory Lists:

We compared the laptop inventory lists provided by Accounting and Finance and ITS SharePoint to determine accuracy and completeness of the laptop encryption process.

- Both Accounting and Finance inventory listing and ITS Sharepoint lists contained records for assets that were listed more than once:
  Accounting and Finance - 17 duplicate records
  ITS - 74 duplicate records.

- Discrepancies between Accounting & Finance Inventory List and ITS Sharepoint List:

				Discrepancies	
	Per A&F	***Per ITS***	***Matched by IA***	***Not listed on ITS SharePoint***	***Listed on ITS but not listed on A&F***
Laptops	2,150	1,166	1,023	1,127	143

  - ➢ At the beginning of the encryption process, ITS identified laptops on their original SharePoint list that were already encrypted or in storage. Even though we requested ITS to identify the laptops removed from the original SharePoint list, ITS was not able to produce this list of laptops; therefore, Internal Audit cannot determine if the 1,127 records mentioned above are included in those records removed from their original list.

- Reconciliation between the Accounting and Finance Laptop Inventory and ITS SharePoint information has not been performed to ensure that all laptops have been properly identified and encrypted.

Recommendation **1:** We recommend that the Information Security Officer (ISO) coordinate with Accounting and Finance and User Support-ITS:

- To work together to reconcile the two asset lists and remove any duplicate records from their lists;

- To determine if the encryption process can be incorporated into the Asset Management module in PeopleSoft to improve efficiency, eliminate redundancy and reduce the possibility of errors by utilizing one asset management application.

Management's Response: The maintenance of multiple lists is not an effective solution as a remediation. OIS will consult with Accounting and Finance the official steward of asset inventory at UTB to develop a consolidated solution for recording the encryption status of laptops. The list maintained by ITS is to be considered a work paper to keep track of laptop encryption services and is not to be considered a document of record.

Implementation Date: Office of Information Security needs to meet with Accounting & Finance to determine the project timeline.

Not able to verify encryption:

We selected a sample of 62 laptops; 50 (80%) were verified as status reported by ITS, 1 (2%) was reported as encrypted and we noted it was not (see Violation of SPB 1), and we were not able to verify the status of 11 (18%) laptops.

Encryption Status Per ITS	Selected	Verified	Not Verified
Encrypted	40	36	4
Missing/Stolen	6	5	1
Pending Encryption	11	5	6
Decommissioned/Hard drive destroyed	3	3	0
Storage	2	2	0
TOTAL	*62*	*51*	*11*

	Encryption Status Per ITS	Reason Internal Audit Not Able to Verify Encryption Status
1	Encrypted	User has laptop and is currently on FMLA.
2	Encrypted	Professor is out of state conducting research. Will return in June 2013.
3	Pending Encryption	Department loaned out to ex-student. Messages left to return laptop. Laptop not returned at the end of audit fieldwork

4	Encrypted	Laptop boxed due to recent office move and department unable to identify which box stores laptop.
5	Pending Encryption	Laptop not found - need to file police report
6	Pending Encryption	Laptop not found - need to file police report
7	Pending Encryption	Laptop not found - need to file police report
8	Encrypted	Laptop not found - need to file police report
9	Pending Encryption	Laptop not found. Possibly same laptop; only transposition of Tag Numbers
10	Reported Missing/Stolen per Dept.	
11	Pending Encryption	Has laptop at home. Has refused to have laptop encrypted.

At the beginning of this audit, 66 laptops were reported as pending encryption on the ITS inventory list, of which we selected 11 laptops for verification; however, we requested an updated status at the end of fieldwork to determine if these laptops were encrypted. Of the 66 laptops initially reported by ITS as not encrypted:

- 1 laptop selected in our sample the user refuses to encrypt the laptop
- 5 laptops selected in our sample are in the process of getting encrypted
- 4 laptops selected in our sample have not been found and departments will file police reports
- 1 laptop selected in our sample is loaned out to a student
- 5 laptops not in our sample have Police Report 1302-00156 dated 5/6/2013
- 50 laptops are still pending encryption at the end of audit fieldwork:

Academic Affairs	44
Provost	1
Research	4
Economic Development	1

See **Recommendation 3** in this report.

Violation of Security Procedures Bulletin 1:

One laptop reported as encrypted on August 10, 2012 was selected for verification. Auditor asked user to reboot his laptop and noticed the encryption software used by the institution was not installed on the laptop. When asked about the different encryption software, the user indicated the laptop has a UNIX operating system and he had personally installed the encryption software. SecureDoc is the encryption software used by the institution that supports both Windows and UNIX/Linux operating systems.

The user did not request an exemption or authorization to remove the encryption software installed by the institution, nor was he allowed to install unauthorized encryption software for UNIX/Linux.

The user violated Security Procedures Bulletin (SPB) 1, which states encryption should be installed "using products and/or methods approved by the Entity's Chief Information Security Officer (CISO or ISO)."

Recommendation 2: We recommend the Information Security Officer coordinate with USS-ITS to ensure that user's laptop is re-encrypted with software authorized by the Information Security Officer.

Management's Response: Office of Information Security will contact the user and coordinate with USS-ITS the re-encryption of the laptop with approved encryption software. All measures will be taken to accommodate the user's needs where compliance can be possible**.**

Implementation Date: : July 1, 2013

See **Recommendation 3** in this report.

Violation of Encryption Mandate:
For one laptop in our sample listed as pending encryption, we contacted the user to verify the laptop encryption status. The user stated he had his laptop at home, it was not encrypted, and would not bring it to get encrypted because encryption would interfere with his laptop's dual boot system (Windows and Linux operating systems). We informed the user about the need and importance of encrypting his laptop. He had been denied an exemption from UT System and was presented with the available solutions offered by the institution, which other UNIX/Linux users had accepted. The user still refused to have the laptop encrypted.

The user is in violation of the requirement to encrypt all University laptops, stated on the memorandum from the Executive Vice Chancellor of Academic Affairs dated June 20, 2012.

Recommendation 3*:* We recommend the Provost/VPAA evaluate the course of action to enforce information security mandates, polices, and procedures, and take appropriate disciplinary action in accordance with UTB HOP and Regents' *Rules and Regulations*.

Management's Response: The Office of the Provost and VPAA concurs with the recommendation. The Provost and VPAA will coordinate with the Office of Human Resources and the Office of General Counsel to insure that all information security mandates, policies and procedures are applied.

Implementation Date: Effective Immediately

Conclusion

The laptop inventory at UT Brownsville is not complete, accurate, and up-to-date due to the discrepancies between the Accounting and Finance Inventory List and the ITS Sharepoint List. In addition, not all institutional laptops have been properly encrypted or exempted in accordance with the UT System Encryption requirement. We could not determine the number of laptops that should be encrypted due to the inaccuracy of the inventory information. Failure to properly encrypt laptops could expose sensitive University data and could lead to costly remediation efforts and negative publicity.