Laptop Encryption Audit

Audit Report # 13-19
October 31, 2013

Office of Auditing and Consulting Services

"Committed to Service, Independence and Quality"
October 31, 2013

Dr. Diana Natalicio
President, University of Texas at El Paso
Administration Building, Suite 500
El Paso, Texas 79968

Dear Dr. Natalicio:

The Office of Auditing and Consulting Services has completed a limited-scope audit of the University’s laptop encryption process. The main audit objective was to determine whether the encryption of laptops is in accordance with UT System and University policies.

We appreciate the cooperation and assistance provided by the management and staff of the Inventory Department, Technology Support, and Information Security Office.

Sincerely,

[Signature]

William A. Peters, CPA, CIA
Director
Report Distribution:

University of Texas at El Paso

Ms. Cynthia Villa, Vice President for Business Affairs
Dr. Stephen Riter, Vice President for Information Resources and Planning
Mr. Richard Adauto, Executive Vice President
Ms. Sandra Vasquez, Assistant Vice President, Equal Opportunity (EO) and Compliance

University of Texas System

Dr. Pedro Reyes, Executive Vice Chancellor for Academic Affairs
Mr. Alan Marks, Attorney, Office of Academic Affairs
Mr. J. Michael Peppers, Chief Audit Executive

External

Governor’s Office of Budget
Mr. Ed Osner, Legislative Budget Board
Internal Audit Coordinator, State Auditor’s Office
Sunset Advisory Commission

Auditors Assigned to the Audit:

Lorenzo Canales (Engagement Manager)
Jerry Montes (IT Auditor)
Paulina Kura (Internal Auditor)
The University of Texas at El Paso
Office of Auditing and Consulting Services
IT Inventory-Laptops

Table of Contents

EXECUTIVE SUMMARY ................................................................. 1
BACKGROUND .................................................................................. 2
AUDIT OBJECTIVE ........................................................................ 2
SCOPE AND METHODOLOGY ....................................................... 2
AUDIT RESULTS .............................................................................
   University-Owned Laptops not Encrypted ...................................... 3
   Laptop Exemption List is not Stored Electronically .......................... 4
   Unencrypted Laptops Missing Exemptions ..................................... 4
CONCLUSION .................................................................................. 5
EXECUTIVE SUMMARY

The audit of the laptop encryption process at The University of Texas at El Paso was conducted at the request of The University of Texas System. The purpose of the audit was to review the University laptop encryption process to determine whether all laptops have been properly encrypted or exempted.

We conclude that the laptop encryption process for the university has been established and implemented; however, we identified laptops which were not encrypted and were not identified as exempt from encryption.
BACKGROUND

The purposes of the University of Texas System Information Security Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices issued on June 1, 2007 are to:

• establish encryption as a requirement in the event that confidential University data are stored on a portable computing device or a non-University-owned computing device, and

• specify practices to ensure that there is a legitimate need before confidential University data are stored on a portable computing device or a non-University-owned computing device and that the owner and user can ensure that encrypted data remain accessible in the event that an encryption key becomes lost or forgotten.

Incidents involving unauthorized exposure of confidential data, such as social security numbers and personal health information, may be the result of stolen or lost portable computing devices and non-University-owned computing devices. The best way to prevent these exposures is to avoid storing confidential data on these devices; however, in situations that require confidential University data be stored on such devices, use of encryption reduces the risk of unauthorized disclosure in the event that the device becomes lost or stolen.

While encryption mitigates risk of unauthorized data exposure, encryption can result in loss of access to the data by authorized users; therefore, procedures to mitigate this risk are also necessary.

Under certain circumstances the Chief Information Security Officer of the entity may grant or issue an exception to the use of encryption on portable computing devices and non-University-owned computing devices containing confidential University data.

AUDIT OBJECTIVE

The objectives of this audit were to evaluate University laptop encryption process to determine whether all laptops have been properly encrypted or exempted.

SCOPE AND METHODOLOGY

The audit scope was limited to laptop encryption processes from September 1, 2011 to March 15, 2013. Audit procedures included interviewing key personnel, reviewing applicable regulations, and verifying the existence of appropriate institutional policies and procedures.

The audit was conducted in accordance with the International Standards for the Professional Practice of Internal Auditing issued by the Institute of Internal Auditors.
AUDIT RESULTS

To gain a better understanding of the process and controls the Office of Auditing and Consulting Services (OACS) conducted a process mapping session and invited campus subject matter experts (SME) to assist in the development of a Visio flow chart. Attendees included SMEs from:

- Inventory Department
- Technology Support
- Technology Implementation Managers (TIMs)
- Information Security Office (ISO)

We mapped the laptop encryption process and identified cross-functional departments which have a stake in the management of University laptops and must comply with encryption policies. Controls were identified for testing to determine whether they are functioning as intended.

**University-Owned Laptops not Encrypted**

Dell, Inc. provides an asset report list of Dell laptops purchased by and shipped to the University. This asset report is automatically e-mailed to the Director of Technology Support. Apple does not currently follow this same process, but all Apple computers are configured by the Technology Support Department and the encryption process is completed at that time. During the testing phase of the audit, University-owned Dell laptops which were tagged and delivered to end-users were found not to be encrypted. Unencrypted laptops could expose sensitive information if compromised.

**Recommendation:** The ISO should request a copy of the Dell Asset report along with an updated inventory report on a regular basis and reconcile to the laptop encryption list. The ISO along with Technology support should develop policy and procedures that all newly acquired laptops be routed to Technology Support to ensure laptops are encrypted prior to delivery to end user.

**Management Response:** ISO is currently receiving the Dell asset reports. These will be loaded into our database for verification that the system has been encrypted. The Dell assets will also be used to verify that the inventory system has the same information we have received.

We will work with Technology Support and the TIMs to determine the best process to deliver new systems and validate they are encrypted.

**Responsible Party:** Gerard Cochrane, Chief Information Security Officer

**Implementation Date:** February 28, 2014
**Recommendation:** Central Receiving should deliver all laptops to Technology Support before delivery to the department, to ensure laptops are encrypted.

**Management Response:** Technology Support is working with ISO to ensure that all newly acquired laptops and desktops are encrypted prior to first-time use. The UTEP standard image has been updated to include the SecureDoc software and testing is being conducted to ensure that hard drive is encrypted prior to anyone is able to logon. Once this corrective measure is implemented, the new computers will start encrypting the hard drive as soon as they are turned on for the first time in UTEP’s network.

**Responsible Party:** Frank Poblano, Assistant Director – Information Resources & Planning

**Implementation Date:** January 3, 2014

**Laptop Exemption List is not Stored Electronically**
The ISO does not store exemptions to the laptop encryption policy electronically. All exemptions are kept on paper file. If the paper copy of the exemption has been lost, destroyed, there would be no evidence of an exemption on file.

**Recommendation:** The ISO should also create an exemption list database on line and make it available on the UTEP Encryption list website.

**Management Response:** Systems will be added to the Encryption Dashboard for tracking of these systems.

**Responsible Party:** Gerard Cochrane, Chief Information Security Officer

**Implementation Date:** December 2, 2013

**Unencrypted Laptops Missing Exemptions**
The list of encrypted/not encrypted laptops provided by the ISO contained 2684 laptops, of which 385 (15%) were labeled as "NOT ENCRYPTED". However, only 5 laptops exemptions were found on file with the ISO. Unencrypted laptops could expose sensitive information if compromised.

**Recommendation:** As soon as a laptop has been identified as unencrypted, the ISO should mandate a department/user has 30 days to have an exemption form on file or encrypt the laptop. The ISO should review the exemption list on an annual basis to ensure the exemptions are still warranted.

**Management Response:** There is a discrepancy from our dashboard of 19% as not being encrypted (Total Devices: 2923 and Encrypted Devices: 2357). We found that our encryption server actually has 2808 systems listed. If we take total encrypted devices in the console and compare that to the total number of systems in inventory we get an encryption rate of 96%.
The reason our dashboard is showing a lower number of computers being encrypted is because we can’t match a serial number from the encryption server to a serial number in inventory. The few we have found have been because the serial number in inventory was not correct.

We will work with our campus departments and colleges to correct the serial numbers in inventory so we can accurately match them to systems in the encryption console.

**Responsible Party:** Gerard Cochrane, Chief Information Security Officer

**Implementation Date:** March 31, 2014

---

**CONCLUSION**

Based on the results of audit procedures performed, we conclude that the laptop encryption processes and controls should be strengthened by implementing the recommendations in this report.

We wish to thank the Inventory Department, the Information Security Office and Technology Support for their assistance and cooperation provided during the audit.