The University of Texas System
Laptop Computer Encryption Implementation – Frequently Asked Questions

Question 1: What audience is this FAQ directed towards?

Answer: This FAQ has been written specifically to address questions that executives, managers, and staff charged with implementation of laptop encryption may have about the directive issued by UT System to the Presidents of all System institutions concerning revised, mandatory laptop encryption requirements.

Question 2: The communication to Presidents indicates that all University laptop computers are to be encrypted by August 31, 2012. Policy at my institution, in compliance with UTS-165 Information Security Bulletin 1, is to encrypt only those laptop computers that contain confidential information. Why has the policy been expanded to include all University laptop computers?

Answer: Encryption of all laptops has always been preferable, given the difficulty of predicting and monitoring what data may be stored on a particular laptop computers. In fact, this is the policy at a number of U. T. Institutions. The world has changed significantly since 2007 when the laptop encryption policy was enacted. Citizens' expectations regarding protection of their privacy have increased, government regulations and penalties have become more stringent, world-wide markets for stolen personal data have developed across the Internet, and occurrence of identity theft has increased. Experience has demonstrated that people do not always know what type of data is contained on their computers and cannot predict with certainty what future data may come to reside on them as roles change and computers are re-provisioned for different purposes. Fortunately, computer encryption software has matured, making encryption easier to deploy and more user friendly. In short, the need for encryption has increased and solutions have become more mature, more affordable, and less burdensome to the user.

Question 3: Experience at our Institution indicates that few, if any, of our data exposures have been result of stolen or lost laptop computers, so why must we make laptop encryption a priority for this institution?

Answer: Development of a consistent, System-wide approach to privacy and security has become a top priority at UT System. Laptop encryption is an essential component of a robust security program and has become a priority for UT System and its institutions.

Question 4: There are strategies other than encryption for protecting data stored on laptop computers. Can other compensating controls be used in lieu of encryption?

Answer: No. Institutions are encouraged to use a defense-in-depth strategy by employing a combination of physical, administrative, and technical controls to protect data stored on laptop computers; however, these other controls are not acceptable substitutions for encryption. Encryption is an essential last line of defense for laptop computers.

Question 5: Lack of resources has posed a barrier to our encryption efforts. How can U. T. System assist?

Answer: The Board of Regents allocated funds to address information security gaps identified by the recent System-wide Information Security Assessment. A portion of these funds has been made available to assist with purchase of encryption software licenses if needed and for hiring contract workers to assist your staff with deployment. Please ensure that your institution's deployment

plan to U. T. System Administration includes any required requests for purchase of licenses or need for supplemental labor to ensure that your institution can meet the revised encryption requirement.

Question 6: How will implementation be tracked?

Answer: These projects will be tracked along with all other projects associated with addressing gaps identified during the Systemwide Information Security Assessment. Because of the short completion deadline for the laptop encryption initiative, weekly status updates will be required until the institution has achieved 100% compliance.

Question 7: At our institution we provide a process through which faculty and staff can apply to have a laptop exempted from the encryption process. Can these exemptions remain in place?

Answer: No, any current exemptions must be reviewed at the System level. Your institution's Information Security Assessment Initiative project plan should identify all exceptions that have been granted and the reasons for those exemptions. Staff within U. T. System Information Security Compliance will confer with your staff to reassess risk posed by all existing exemptions. Exemptions will be rare, and allowed only under circumstances that pose extremely low risk, are thoroughly documented, and must be individually authorized by the President of the institution.

Additional Information: Exemptions submitted to UT System for review must provide the following information for each device for which an exemption is requested: 1) an individual identifier for the device (e.g. one of the following: inventory number, MAC address, serial number etc.), 2) the owning department and/or location of the device, 3) current use of the device, 4) reason why encryption cannot be performed, 5) reason that the device cannot be retired or replaced, 6) any compensating controls that are in place or proposed.

A visible label must be attached to all University owned/leased computers that are exempted from encryption. The label must state something to the effect of: "WARNING: This device is not encrypted. DO NOT place confidential University information on this computer. To do so is a serious violation of University policy." Wording can be modified to meet the needs of the circumstances, keeping in mind that the purpose of the label is to alert staff that the device must be encrypted if repurposed.

Question 8: To achieve compliance, is it acceptable for faculty, researchers, and staff to select their own method of encryption?

Answer: No. Encryption products and process are not all of equal quality and reliability. Only "whole disk" or equivalent encryption solutions that can be verified as being in place following loss of a computer are acceptable. When a device becomes lost, it is essential that the Institution be able to state with assurance that all data residing on the laptop is encrypted. Otherwise, if confidential information resides on a device that becomes lost, the data must be considered to have been exposed, and all regulatory notifications requirements must be met. This creates business disruption and additional cost.

Question 9: Laptop computers are but one of a number of types of mobile devices being used within U. T. Institutions. Why is initial focus being placed on laptop computer encryption rather than encryption of devices such as mobile phones and tablet computers?

Answer: Laptop computers tend to be used for storage of much larger sets of data, including spreadsheets and databases used to support business functions. These files often hold thousands of individual records and can pose high risk. Cell phones, tablet computers, and other personal data devices, at present, tend to be used for more transient information such as email. While all these devices pose risk, at present, the laptop computer represents a higher, risk. Also, the U. T. System policy framework and software for laptop computer encryption is more mature, making it easier to implement solutions for this platform at present.

These other devices will be addressed. In response to the Systemwide Information Security Assessment audits, U. T. System is working with subject matter experts from System institutions to develop policy and to select appropriate software for managing security of mobile phones and tablet computers. Also, System is in process of making highly secure, encrypted USB drives (i.e. thumb drives) available to faculty so they will always have a secure means of transporting data in a manner that will pose minimal risk were the device to become lost or stolen. Additional information about each of these initiatives will become available before end of summer.

Question 10: The communication to Presidents makes reference to encryption of desktop computers. What are the requirements and timeframes for this effort?

Answer: Requirements and timeframes for deployment will be issued during September 2012. Policy is still under development.

Question 11: What about encryption of data on personally owned computers used at home?

Answer: The best practice is to educate your faculty and staff that all data they collect and maintain in their roles as University faculty and staff is the University's data and they should avoid placing any University data on personal home computers. U. T. System institutions have experienced a number of incidents over the past few years in which homes have been burglarized and computers holding sensitive University data have been taken resulting in data exposure. All U. T. institutions have technology and processes in place that allow for secure access to office resources remotely. Use one of these methods. Alternatively, use a University provided encrypted USB drive (see answer to Question 9) to hold data that needs to be transported securely to another location.

Additional Information: It is imperative that all employees know that there is to be no confidential data downloaded to a portable or personally owned computer without permission of the data Owner, and any such data must be encrypted using Institutional ISO approved methods. This is current policy, and has been so since June 1, 2007, as stated in Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices (http://www.utsystem.edu/ciso/documents/SPB1.pdf). Owners are responsible for the data under their authority and must be very cautious when assessing risk to data when deciding whether to grant permission for download.

Following are pertinent policy provisions from the UTS-165 Security Practice Bulletin #1 Expectations Section:

1. As a general practice Confidential University Data are not to be copied to or stored on a Portable Computing Device or a Non-University Owned Computing Device.
2. Specific permission must be obtained from the data Owner before a User may store Confidential University Data on a Portable Computing Device or a Non-University Owned Computing Device. Such permission should be granted only upon demonstration of a business need and an assessment of the risk of unauthorized access to or loss of the data.

3. Any Confidential University Data stored on a Portable Computing Device or Non-University Owned Computing Device must be encrypted using products and/or methods approved by the Entity's Chief Information Security Officer (CISO or ISO).

After receiving Owner permission, it is the requestor's responsibility to see to it that the device is encrypted in accordance with Institutional requirements. The Institution must either encrypt the device or otherwise verify and document that the device is properly encrypted.

Question 12: We have been instructed to send implementation plans to UT System via email. Should I be concerned about sending this by email since the plan will contain sensitive information about the institution's security posture?

Answer: Risk is mitigated because email exchanged between System and the primary email server at each UT campus is automatically encrypted during transmission. This capability has been in place since October 2011 as result of System collaborating with the email administrators at each UT Institution.

Question 13: I have additional questions. To whom should these be addressed?

Answer: Submit inquiries to ciso@utsystem.edu, or contact Lewis Watkins, UT System Chief Information Security Officer at (512) 499-4540.

Question 14: What about student computers?

Answer: The requirement for encryption does not include student computers unless a student is also serving in a role results in confidential University data being stored on the computer.

Question 15: Must a home computer be encrypted if it is used by an employee to remotely connect to an office computer to perform work in a way that ensures that all processing and file storage is conducted on the office computer rather than the remote computer.

Answer: If all business processing and file storage is isolated to the office computer, encryption is not required on the remote computer because data is not at risk. However, it is imperative that the institution understand and communicate to its employees which of the remote access methods made available by the institution meet this criteria. If other methods that do not meet this criteria are also used on the remote computer, the remote computer must be encrypted.