

U. T. System Security Practice Bulletin 1 - Frequently Asked Questions

Encryption Practices for Storage of Confidential University Data on Portable and Non-University Owned Computing Devices

<p>Q-1. Why must we use encryption on portable and non-University owned devices containing Confidential University Data?</p>	<p>A. Today’s university environment is complex and data is stored in many places including portable devices, and in some cases perhaps home computers. Unfortunately, these devices are easily lost and stolen. We hear about such incidents weekly in the news. Within the University of Texas System there have been lost and stolen laptops and USB (“thumb” or “stick”) drives and employees who have had home computers stolen. The devices contained confidential information such as student records, employee information, patient information and/or research data. The risks are real and proven. A lost or stolen device that is properly encrypted poses virtually no risk of exposure of any confidential information that may reside on the device. U. T. System institutions must raise the bar in terms of protecting confidential information in order to ensure we maintain an ability to meet instructional, research, patient care, and public service missions. Use of encryption will ensure better protection of confidential information and help maintain public trust.</p>
<p>Q-2. Must all laptops, portable devices and non-University owned devices be encrypted?</p>	<p>A. The bulletin applies to portable and non-University devices that contain Confidential University Data. Some U. T. institutions may extend these requirements. Check with your institution’s Chief Information Security Officer (CISO or ISO) for specific requirements at your institution.</p>
<p>Q-3. Are there alternative ways to accomplish work tasks and protect this information without use of encryption?</p>	<p>A. Yes alternatives do exist, and the very best way to prevent Confidential University Data from being placed at risk on a lost or stolen portable device is to never place such information on portable devices! If confidential data absolutely must be placed on a portable device, it should not be stored there on a permanent basis. It should be removed as soon as it is possible to do so.</p> <p>In some cases work can be accomplished by using only a subset of data that may exclude the confidential portion of the data. Think about the information actually needed to accomplish your goal and avoid downloading any unneeded data.</p> <p>Also, look for alternative ways to achieve your work goals. Rather than placing confidential data on a laptop or portable storage drive, ask your Information Technology department about possible use of remote access solutions. Through mechanisms such as Virtual Private Networks (VPN) or Remote Desktop Services technologies, you may be able to access data remotely to accomplish your work without having to actually store the data on a portable device.</p>

<p>Q-4. Under what authority is this encryption bulletin being issued?</p>	<p>A. <u>The Information Resources Use and Security Policy (UTS165)</u> authorizes the UT System Chief Information Security Officer to issue security practice bulletins relating to standards and best practices in order to allow the University to respond quickly to emerging information security threats.</p>
<p>Q-5. How does encryption work?</p>	<p>A. Encryption is simply a way of scrambling the contents of a document, file or message so that only the owner, or in the case of email the recipient, can unscramble its contents. The ingredients for encryption are: 1) the text of the document/message, 2) an encryption “key,” and 3) mathematical algorithms used with the text and key to create the scrambled document, file, or message. Using the key, the owner or recipient can unscramble the document.</p>
<p>Q-6. How complex will this be for me to use?</p>	<p>A. There are various solutions with varying requirements. Many U.T. institutions are deploying what is called “whole disk” encryption to address the specific needs of this bulletin. Whole disk encryption solutions are for the most part “transparent” to the user during daily use. When first installed to a person’s computer, the encryption software does take a long time (perhaps several hours) to encrypt the computer’s whole disk drive. When this one-time operation is accomplished, however, the whole disk encryption is maintained in the background while the computer user goes about normal work tasks. For most workers, the overhead performance impact is negligible (3% to 5%) and not noticeable. If the computer becomes lost or stolen there is no need for concern about exposure of any confidential data that may reside on the computer.</p>
<p>Q-7. My laptop computer requires a logon ID and password for access. Why is this not sufficient protection?</p>	<p>A. While an ID and password combination provides a very basic level of protection, it does not prevent someone who has possession of the device and who is determined to access your data from doing so. The ID and password simply prevent them from accessing the files in the manner in which you would normally access them. The files on the disk drive are stored in what is called “clear text” format. With specialized skills and software, there are ways to access the files without use of the ID and password. Remember, the best protection is to not hold confidential information on portable devices. But if you must store confidential data on such devices, it must be encrypted to be adequately protected from unauthorized exposure.</p>
<p>Q-8. I know nothing about encryption; who can help me with this?</p>	<p>A. Contact your institution’s Information Security Office (CISO or ISO Office) for assistance.</p>

<p>Q-9. Is any encryption solution ok, or must I use a specific product?</p>	<p>A. Contact your institution's Information Security Office for guidance about recommended and/or supported solutions.</p> <p>It is important to know that not all encryption products are made equally. There are different strengths of encryption. Encryption strength is a function of the mathematical algorithms used and the length of the encryption key.</p> <p>In the event of lost or stolen devices containing confidential information, it is important to be in a position to unequivocally assure the University and the public that there is no possibility of confidential information being exposed. By using products recommended by your Information Security Office, you will be in a position to do so.</p>
<p>Q-10. What if funds are not available to provide the needed encryption software?</p>	<p>A. A variety of solutions exist, some of which are open source and have no cost. Cost for one product being used at some U. T. institutions is about \$28 for each user license and less than \$4.50 for annual maintenance.</p> <p>When considering encryption solutions, be sure to use solutions that are recommended and/or supported by your institution's Information Security Office and consider the cost of the encryption solution versus the potential risk of exposure of the confidential data. A database containing hundreds or thousands of records with confidential information such as social security numbers can, if lost or stolen, cost the University tens or hundreds of thousands of dollars to address the incident. This does not include hidden costs such as loss of reputation and public confidence leading perhaps to reduced donations and jeopardy of research grants. If an investment of less than \$50 is not possible to offset the potential liability, alternative ways should be considered for addressing the work situation. Explore the possibility of completing the work in the University office setting rather than using a portable device or explore using remote access capabilities that do not require placement of the data on a portable device.</p>
<p>Q-11. I believe I have a unique situation that warrants an exception to the encryption requirement; who should I contact to discuss this?</p>	<p>A. Contact your institution's Chief Information Security Officer (CISO or ISO).</p>

<p>Q-12. Does use of encryption itself pose any risks?</p>	<p>A. The primary risk with use of encryption is that the key required to decrypt (unscramble) encrypted data might become lost or corrupted making it impossible to access the encrypted data. Another possibility is that the person who encrypted the data may leave the University or could even die, making it impossible for the University to gain access to the encrypted data.</p> <p>There are methods to mitigate these risks. The best safeguard is to use a sound data backup procedure. Under most circumstances data stored on a portable device should not be the primary data source but simply a copy of data that resides on a secure storage device or server maintained by the institution. If a laptop or other portable device is stolen, or destroyed, or if the encryption key is lost or stolen, the data will be still be accessible because it is also stored on the University's secure server. Another approach is called key escrow which simply means that another authorized party such as the Chief Information Security Officer has a copy of the encryption key.</p>
<p>Q-13. On occasion I must store Confidential University Data on my home computer. Must it also be encrypted?</p>	<p>A. It is seldom a good idea to store Confidential University Data on a personally owned computer. However, if for some reason it is to occur, then the stored information <i>must</i> be encrypted. The risk to the University is just as great when data is stored on a personally owned computer as when it is stored on a University owned computer. There have been incidents in which personally owned computers containing Confidential University Data have been stolen from an employee's home.</p>
<p>Q-14. I check my University email from home. Does this pose any risk?</p>	<p>A. If you receive email messages or attachments that contain Confidential University Information, depending on how your email is set up, the computer you use from home may be holding files that contain Confidential University Information. This can be true even if you use the web to access your work email. As a precaution you should regularly delete temporary files and temporary Internet files.</p>
<p>If you have additional questions, please send them to: ciso@utsystem.edu</p>	