

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

Q-1. Why must we use encryption on portable and non-University owned devices containing Confidential University Data?	A. 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.
Q-2. Must all laptops, portable devices and non-University owned devices be encrypted?	A. The bulletin applies to portable and non-University devices that contain Confidential University Data.
Q-3. Are there alternative ways to accomplish work tasks and protect this information without use of encryption?	A. With 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.
Q-4. Under what authority is this encryption bulletin being issued?	A. <u>The Information Resources Use and Security Policy (UTS165)</u> authorizes the UT System Chief Information Security Officer to issue policies to allow the University to respond quickly to emerging information security threats.
Q-5. My laptop computer requires a logon ID and password for access. Why is this not sufficient protection?	A. 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.
Q-6. Is any encryption solution ok, or must I use a specific product?	A. Contact your institution's Information Security Office for guidance about recommended and/or supported products. It is important to know that not all encryption products are made equally. There are different strengths of encryption. In the event of a lost or stolen device containing confidential information, it is important to be in a position of being able to unequivocally being able to 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>Q-7. 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. One 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-8. 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.</p>
<p>Q-9. 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: infosecurity@utsystem.edu</p>	