The University of Texas System

University Owned Desktop Encryption
Requirements and Frequently asked Questions

Desktop Encryption Requirements:

1) High risk desktop computers are to be encrypted by May 31, 2014.
   a. Deans, Chairs, and/or Department Heads, in concert with the institution's Chief Information Security Officer are responsible for identifying the desktops in their areas that are high risk, based on guidelines included in this document.
   b. All other desktop computers may remain unencrypted until they are replaced following the respective institution's guidelines for hardware refresh and replacement, at which time they would be properly disposed.
2) All new desktop computers purchased on or after September 1, 2013, are to be encrypted before deployment. Where budgets allow, self-encrypting drives should be purchased by default with encryption enabled.

Desktop Encryption Process Management Requirements:

1) The institution must implement processes for tracking and documenting the encryption status of desktop computers in order to know the encryption status of a device were it to become compromised, lost or stolen, and for reporting implementation progress.
2) The institution's Chief Information Security Officer shall create a plan that, at minimum, describes the following, and **forward this plan to ciso@utsystem.edu by June 1, 2013.**
   a. the process the institution will use to identify high-risk desktop computers.
   b. the process the institution will use to determine the priority and order in which the high risk computers will be encrypted.
   c. the tools and/or processes to be used to monitor the encryption status of desktop computers.
   d. the processes to be used to ensure that desktop computers purchased beginning September 1, 2013 will be encrypted prior to deployment.
3) The institution will provide periodic progress reports as requested from UT System.

The University of Texas System
Desktop Encryption Frequently asked Questions (FAQ)

Question 1: What is a "high risk" desktop computer?

Answer: In general, there are three circumstances that indicate that a desktop computer is high risk. These are as follows:

Based on Location: Desktops in public/high-traffic areas that are used by staff with access to confidential/protected data are considered high risk. Small form factor desktops pose an additional risk.

Based on Business Function: Desktops may be high risk based on the activities of the business unit in which they are located. For example, desktops in clinical, hospital, or HR settings are likely high risk because of the type of work performed in these functional areas. The business unit function/area centric approach is the easier to implement because it does not require risk-scoring every desktop in the environment.

Based on Role of User: Computers belonging to Executive Officers and their support staff should, by default, be considered high risk as the loss of these computers will likely have an adverse impact on the reputation of the individuals as well as the institution as a whole.

The criteria outlined above are not all inclusive. Any desktop computer on which data is stored that if accessed by an unauthorized party or that holds data that if subject to unauthorized change or deletion would have highly adverse impact on the University is high risk

Question 2: Who makes the final determination as to whether a desktop computer is to be considered high risk?

Answer: The decision is made by management of the functional area where the device is located in consultation with the Institution's Information Security Officer and based on criteria identified in the answer to question 1 above. If a dispute arises, the Information Owner of the data placed at potential risk will determine the classification of the device, in accordance with Information Owners responsibilities as outlined in TAC 202.71 (1)(A through I). Any resulting information security exception request will be documented and reported in accordance with the institution's existing process for handling such requests.

Question 3: Is there a date by which all high risk desktop computers must be encrypted?

Answer: Yes, May 31, 2014.

Question 4: Is there a date by which all other desktop computers must be encrypted?

Answer: There is no single date that applies to all other desktop computers. However, any desktop computer purchased on or after September 1, 2013 must be encrypted.

Question 5: Are there any desktop computers that do not have to be encrypted?

Answer: Yes, desktop computers that meet the following criteria do not require encryption because they do not retain data. Note, however, documented exemptions are required for these computers.

- Computers that have software controls in place such as "Deep Freeze" to enforce data wiping after each use.
- Kiosk computers that are designed not to store any data locally (including browser caches).
- Network bootable computers designed with no local hard drives.
- Virtual desktops for which the hypervisor is a secure "cloud service" and does not permit transfer of the virtual image. Note: If the hypervisor itself is a desktop computer, then the desktop itself should be encrypted.
- Thin clients that have no local storage.

Question 6: Are any other exemptions possible?

Answer: Circumstances may exist that prevent use of encryption on some computers. In such situations an exemption will be considered. Exemption requests are processed as follows:

Step 1:	**Exemption Documentation:** The Requestor documents in writing the need for an encryption exemption. Requests must include the following information: 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 to mitigate risk. 7) any supplemental documentation that may exist in support of the request such as vendor literature or analysis and recommendations from faculty or colleagues.
Step 2:	**Request Submission:** Requestor submits the exemption request to the institution's Information Security Officer (ISO) for review and consideration. (Expected turnaround time for decision would be within two weeks of submission.)
Step 3:	**Decision Process:** Institutional ISO makes decision based on the documented need and the associated risks. • The ISO has the option of forwarding the exemption request to the UT System CISO for review and opinion or decision. Response from the UT System CISO, including an explanation of the recommendation or decision, will be sent to the campus ISO within three days of receipt of the request at UT System.
Step 4:	**Communicate the Decision:** **Approved Requests:** If the exemption request is approved, the ISO assigns an expiration date for the exemption and notifies the Requestor of the approval. • If an extension beyond the expiration date is needed, a request for extension must be submitted to the ISO. • All approved exemptions must be reported to the President in the Information Security Program Annual Report to the President. **Denied Requests:** If the ISO denies the request, the ISO informs the Requestor and the President of the denial and provides an explanation for the denial. • The President may accept the decision of the ISO, override the decision, or request additional information or actions to be taken in order to reach final decision.

Note: The exemption process outlined in Question 6 applies also to exemption requests for laptop computers and mobile devices that are University owned or are personally owned but that contain University information that meet requirements for encryption.