The University of Texas System
Encryption Requirements for Personally Owned Computers

Requirements:

A personally owned computer must be encrypted if it contains any of the following types of University information[1]:

1. Information made confidential by federal or state law, regulation, or other legal agreement.
   This includes, but is not limited to, data protected by FERPA, HIPAA, the Texas Public Information Act, and the Texas breach reporting law (Business &Commerce Code Section 521.002(a)(2)).
   Examples: education records, patient medical treatment and payment records, Social Security Numbers, credit card numbers.
2. Federal, state, university, or privately sponsored research that requires confidentiality or is deemed sensitive by the funding entity.
3. Any other information which has been deemed by the UT System or a UT System institution as essential to the mission or operations of System to the extent that its integrity and security should be maintained at all times.

Background and Guidance: The following information is provided for explanation and guidance only.

✓ **Understand why encryption of laptop computers and home computers is important:**

- **Data Exposure Reality:** Within the UT System institutions, most incidents of unauthorized exposure of University data have been result of lost or stolen laptop computers, thumb drives, and people's home computers.
- **Consequences of Data Exposures:** Data exposures cause real harm to people and to the University. Exposure of a person's confidential information can result in identity theft and/or great embarrassment to the individual. At minimum, data exposure incidents create anxiety for those impacted. The University suffers financial loss resulting from costs of investigations, mandatory notifications, credit monitoring services, and potential fines. For faculty, data exposures can result in theft of their research and intellectual property. Incidents also cause reputational harm to the University as well as to the departments and individuals responsible for the data loss.
- **The Human Factor:** People understand that unfortunate events will occur, but each person tends to believe such events will happen to someone else and not themselves. Just as nobody expects to have an auto accident on any specific day, nobody expects to have a computer or thumb drive stolen or lost. Over time, however, each person is likely to be involved in an accident and also to have a device lost or stolen. Safeguards must be put in place prior to occurrence of the unexpected event. As owner of a device you hold the key to securing data under your control.

✓ **Do Not store University data on your personally owned laptop or home computer.** Best practice is to use only University owned computers for University business. However, if you do elect to store University data on a personally owned device, the encryption requirements above must be followed.

✓ **Do Not rely on encryption alone.** Encryption is effective only when used in conjunction with other safeguards. Use a strong password to protect your computer and turn the computer off when it is not in use. If the computer is on and you have logged on already when it is stolen, the computer operates as if you are the one using it. Encryption provides no protection in this situation, so always turn the computer totally off when it is not in use.

✓ **Backup data frequently.** Data backups are needed for a variety of reasons. Computer storage, whether encrypted or not, can become corrupted making your data inaccessible. Also, if your computer is lost or stolen, you want to make sure you have not also lost your data. Backing up data to a University computer or server provides protections in these situations.

✓ **Give careful thought to your encryption password.** The encryption password must be complex, but also one that will not be forgotten. Without the password you will not be able to access your data unless the data is backed up in an unencrypted state elsewhere. Consider storing the password in a software vault on a separate device or, if written, store the password in a location well removed from the computer and do not identify it as a password.

✓ **Contact your campus Information Security Office if you have specific questions about encryption software and practices.**

[1] "University information" means all recorded information created or received by or on behalf of the University (or System) that documents activities in the conduct of state business or the use of public resources. This includes all information generated by a University employee in the course of performing his or her duties regardless of whether it was created and/or located on a personal device owned by the employee.