Confidential information that is stored on Texas State-owned laptops must be protected by encryption. Encrypting laptops helps ensure that confidential information does not fall into malicious hands. Texas State has chosen McAfee Endpoint Encryption for Windows laptops and FileVault 2 for Mac laptops as the approved and supported encryption solution. Both encryption solutions are highly rated in the security industry, are enabled when at rest, and provide minimal impact to the laptop owner.

Understanding Laptop Encryption

Encryption (or whole disk encryption) protects information on laptops from unauthorized access by converting the data into unreadable code that cannot be easily deciphered. This protection is more extensive than typical security features, such as securing your computer with a password or encrypting individual files.

Your laptop is encrypted when the data is at rest or the device is powered off. When encrypted, the data is encoded in such a way that it is not readable. When you log in and access a file, the data is no longer at rest and becomes readable. When you successfully log into your laptop, your data immediately becomes unencrypted and available for you to complete your work tasks.

Laptops are only protected when locked and must require login credentials to access the device. McAfee Endpoint Encryption settings lock Windows laptop screens after 15 minutes of inactivity (e.g., no keyboard use or mouse clicks). If a laptop is unlocked and inactive, the data is unprotected, vulnerable, and in an unencrypted state. On Mac laptops, once FileVault2 is installed, laptop owners who did not previously log into their computers will be required to provide login credentials to access the device.

If the laptop is lost or stolen, an individual cannot access your encrypted data without a valid username and password. To access your specific data, the person would have to be an administrator on the laptop or have your login information. If the hard drive is removed from the laptop, it is considered at rest and protected by encryption.

Laptop Encryption and Backing Up Confidential Information

When thinking about backing up software, keep this in mind: Any data that is copied to an unencrypted external device or location is not encrypted and will not be protected. Texas State policy does not allow the storage of confidential information in an unencrypted location.

Examples of acceptable external storage devices for university confidential information:
- Encrypted thumb drive or flash drive (e.g., IronKey)
- Encrypted external hard drive (e.g., Apricorn Aegis Padlock)

Staying Connected and Protected

Due to laptop mobility and a higher likelihood of being lost or stolen than desktop computers, Texas State is only requiring that laptops be encrypted. Some high-risk desktop computers may also be candidates for encryption. Contact the IT Assistance Center if you have concerns about desktop computers that fit this need.

Exceptions can be made for lab laptops that are managed in a way that automatically removes users’ saved data after reboot. For example, using DeepFreeze software any data that someone recently saved will be removed immediately when the computer is restarted.

Learn More about the Texas State Laptop Encryption Program

The IT Assistance Center will contact each department to begin the encryption process. Learn more about the encryption campus adoption plan on the Laptop Encryption Program website.