College of Communication Computer Encryption

University of Texas Data Security Policy

In order to comply with University policies regarding data security, all University owned laptops and desktop computers are required to be encrypted. This policy was initially enacted to cover laptops but has been expanded to desktops as well. Few exceptions are granted to this rule given the likelihood of sensitive data being stored on such devices. College computer labs are one example of systems that are granted exceptions.

There are a few methods by which this can be accomplished. Some across the University utilize a software encryption tool called SecureDoc. The College of Communication TechTeam works with encryption methods already built into the Windows and MacOS operating systems, namely, Bitlocker and Filevault. New systems are encrypted as they are provisioned and before being deployed. All existing laptops have been encrypted per this policy and desktops are being completed as new ones arrive or as they are rebuilt.

The service complies with the requirements for protecting portable devices, outlined in the Information Resources Use and Security Policy, Section 5.20. This policy is also highlighted in the Minimum Security Standards for Data Stewardship (PDF).

If you have a university owned computer or know of one that is not encrypted, please contact the College of Communication Technology Staff to make sure it is remedied as soon as possible.

Patron Responsibilities

Technology Services patrons agree to adhere to the university's Acceptable Use Policy and will manage data in responsible manner. In addition, patrons of College of Communication technology resources will abide by university encryption policies for laptop devices.

Patrons agree that Technology Services administrative accounts will be maintained on all supported systems and that access to those systems. Technology Services will not access offices, work systems or network shares unless required for troubleshooting a specific problem or security risk.