**Research Data Management Best Practices**

ETSU’s Digital Research Data Storage and Backup Policy requires that researchers back up data on secure ETSU network drives or on ETSU OneDrive for Business. HIPAA data may not be stored on ETSU OneDrive for Business but must be stored on ETSU’s HIPAA-compliant network drive, HIPAA-compliant REDCap server, or HIPAA perimeter within the ETSU AWS cloud. HIPAA data stored in these locations are encrypted in transit and at rest. ETSU network drives are backed up daily by ITS Systems Support. ETSU electronically enforces a strong password policy and two-factor identity authentication on network connections. Out-of-support operating systems are blocked from the network. The ETSU guest network is separate from the main ETSU network.

ETSU Research Computing Services strongly recommends LastPass password management in support of complex password creation and device encryption. ETSU Mac computers are protected against malware, viruses, and other vulnerabilities with Cisco AMP and PC’s are protected with MS Endpoint Protection; updates are installed automatically. ETSU Research Computing Services recommends the use of ClamTk Antivirus with automatic updates on Linux machines. Laptops are encrypted per Tennessee State law upon arrival at ETSU. Desktop encryption is not currently mandatory but is possible through FileVault on Mac’s and BitLocker on PC’s. Containers or partitions may be encrypted on Linux machines with VeraCrypt. While platform specific flash drives may be encrypted with FileVault or BitLocker, cross-platform flash drives are encrypted with VeraCrypt or hardware encrypted flash drives are purchased. A disaster recovery plan and incident response plan is in place for restoration of network services. Data lost from ETSU-ITS network drives and storage areas through drive failure or accidental deletion can be restored for up to 20 days. Research Computing Services strongly recommends activation of device locator software for laptops and mobile devices. Secure authenticated data sharing is possible through MS Outlook e-mail encryption, ETSU OneDrive for Business, and the ETSU REDCap servers.