Policy Title: Portable Computational Device Security Guideline

Policy Type: Technology **New/revised:** Revised

Old Policy #: Portable Computational Device Security Guideline

Approval level: ☐ Board of Trustees
☒ President
☐ Vice President
☐ Other (specify here)

Purpose: This guideline provides recommendations to safeguard sensitive information stored on laptop computers, smartphones, removable media, and other mobile devices such as iPads and tablets. The guideline should be followed by ETSU faculty, staff, students, contractors, consultants, temporaries, and other workers including all personnel affiliated with third parties with access to sensitive university information.

Policy:

Smartphones:

ETSU systems automatically enforce security controls to faculty and staff phones connected to the university email system. Use the following tips to provide additional security to your smartphone:

1. Record the phone serial and MAC address number. It may help recover it if lost or stolen.
2. Update your device operating systems and applications as soon as an update is available.
3. Backup your device. When possible enable backup encryption to protect your backups.
4. Enable the phone geo-location and remote wipe capabilities in case it is lost or stolen.
5. Consider using the “if found lock screen” or provide basic owner info in case it is lost.
6. Turn on device encryption and encrypt both fixed and removable storage.
7. Enable screen auto-lock and configure a reasonably short timeout period.
8. Require the use of fingerprint or a password to unlock your phone.
9. Disable unused services, such as Bluetooth, NFC, etc.
10. Consider installing a mobile device antivirus.

Laptops:

ETSU provided laptops are configured with multiple security controls such as password, firewall, antivirus, full disc encryption, etc. Use the following tips to verify and provide additional security to your personal laptop:

1. Record the laptop serial and MAC address number. It may help recover it if lost or stolen.
2. Keep the operating system up-to-date by ensuring the auto-update feature is turned on.
3. Keep third party applications up-to-date and enable their auto-update when available.
4. Enable screen auto-lock and configure a reasonably short timeout period.
5. Ensure the laptop is using an up-to-date antivirus and antivirus-definition.
6. Require the use of a strong password or passphrase.

7. Verify that your laptop hard drive/s are encrypted.
8. Verify that your firewall is enabled.

Removable media:

Removable media such as external hard drives, flash drives and SD cards can be easily lost or stolen. Use the following tips to secure such devices:

1. Consider labeling the device with the owner's information in case it is lost or stolen.
2. Use encryption to protect sensitive data.

Notes:

Approved: Information Technology Governance Council
Updated: May 2016
Reviewed: February 2017

3/24/2017 – approved by the Board of Trustees.