Purpose:

The purpose of this administrative process is to identify HWCOE requirements for managed disk encryption on UF-owned laptops.

Scope:

This administrative process applies to all UF-owned laptops within the HWCOE.

Standard:

1. Laptops must have full-disk encryption enabled that meets UF’s Mobile Computing and Storage Devices Policy and Standard.

2. HWCOE will achieve compliance to UF’s Mobile Computing and Storage Devices Policy on laptops by requiring the encryption management and reporting tools provided in the UF Endpoint Management (UFEM) suite.

3. Encryption status on laptops must be audited by Unit IT.

Please Note: This administrative process requiring the use of UFEM provided tools is only for compliance to UF’s encryption policy. The use of other features of UFEM is at the discretion of Unit IT.

Responsibilities:

1. UFIT will provide a suitable product that meets or exceeds this administrative process as part of its UF Endpoint Management (UFEM) suite.

2. Engineering Business Services (EBS) will assist Unit IT in the on-boarding (use and configuration) of UFEM.

3. Engineering Business Services (EBS) will produce an encryption compliance report monthly for HWCOE UF-owned laptops using the UFEM. The report will be provided to Unit IT for auditing purposes.

4. Unit IT will support UFEM on UF-owned laptops in their unit.

5. HWCOE workforce members will work with Unit IT to ensure UFEM is installed for encryption management on UF-owned laptops and will not uninstall, turn-off, or otherwise disable it or decrypt the laptop unless properly documented and approved within the UF Integrated Risk Management (IRM) framework.

References

UF’s Mobile Computing and Storage Devices Policy and Standard (available at https://it.ufl.edu/policies)

UF Endpoint Management (UFEM) - https://it.ufl.edu/ufem/