UF Herbert Wertheim College of Engineering
UNIVERSITY of FLORIDA

IT Administrative Procedure:
IT2-2-0 Managed Encryption Requirement for Laptops

Purpose:

To identify HWCOE requirements for managed disk encryption on UF-owned laptops.

Scope:

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 regularly.

4. UF-owned laptops not capable of using UFEM tools, or another approved method, for encryption management must complete a risk assessment according to the UF Integrated Risk Management (IRM) framework.

Responsibilities:

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

2. The College IT Director will provide Unit IT a monthly encryption compliance report for auditing purposes.

3. Unit IT will support UFEM on UF-owned laptops within their unit.

4. HWCOE employees assigned a UF-owned laptop will work with Unit IT to ensure UFEM is installed for encryption management and will not uninstall, turn-off, decrypt, or, otherwise, disable it.

References

- *UF's Mobile Computing and Storage Devices Policy* and *Standard*
  https://it.ufl.edu/it-policies/

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