UF UNIVERSITY of FLORIDA
Information Technology

Documentation of Non-Standard Device Encryption

The University of Florida Mobile Computing and Storage Device Security standard requires that all mobile computing devices used in connection with University business implement whole-disk encryption that meets certain specifications. Information on compliant encryption methods can be found at: https://security.ufl.edu/mobilesecurity.

If no compliant encryption product or mechanism is available for a particular device, it still must be encrypted. Until a method that complies with all standards becomes available, another whole-disk encryption method may be used. Once a suitable method that complies with all the requirements in the standard becomes available, the non-standard encryption must be removed and the compliant solution installed.

This form must be completed for each device that utilizes non-compliant encryption methods. This completed form must be retained by the unit for 10 years.

Device brand:_____ Device model:_____

Device serial number: _____ UF asset tag (if applicable): _____

Device Operating System: _____ Version: _____

Owner of the device (either UF or an individual): _____

Name of primary device user: _____

UF unit providing the encryption service: _____

Individual performing the encryption installation: _____

Encryption software used (name, vendor and version): _____

I have encrypted the device described above with whole disk encryption software.

_____ _____

Signature Date