UF UNIVERSITY of FLORIDA
Health Science Center

Security Program for the Information and Computing Environment

POLICY

Policy: TS0010	Category: Technical Security	Version Date: 2/05/2007
Title: Portable Computing Device and Media Security		Effective Date: 2/07/2007
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 2/2007
Review Resp: HSC Chief, Information Security		Next Review: 2/2008

Purpose:

The purpose of the Portable Computing Security Policy is to establish safeguards for the use of portable electronic media and computing devices, including their connection to the network. Portable computing devices include but are not limited to Portable Digital Assistants (PDAs) or Smart Phones such as the Blackberry, Palm, HP (iPAQ), Dell (Axim) and other manufacturers' handheld computer product lines; include notebook or laptop computers, and Tablet PCs; include text pagers and other similar devices capable of capturing, processing, storing and transmitting electronic information. Portable media includes, but is not limited to, compact disks, digital video disks, memory sticks, floppy disks, removable disk drives etc. The portability offered by these devices and media increases the risk of unauthorized disclosure of information stored on them.

Scope:

This HSC Portable Computing Security Policy applies to all individuals that use portable computing devices and media, whether UF HSC issued or privately owned, to access the HSC Information and Computing Environment.

Reference:

SPICE Standard TS0010.02 Portable Computing Device Security

Policy:

1. All other appropriate UF and SPICE security policies applicable to desktop or workstation computers apply to portable computing devices.
2. Users who have a need to store Restricted information on a portable computing device or media must have expressed written authorization by the Unit Dean, Director or Department Chair or his/her delegate to remove such information from the University premises. This authorization must have an expiration period commensurate with the project's duration which may not exceed 24 months. If the project will extend beyond 24 months, the authorization must be renewed biannually.

3. All UF issued portable computing devices, including those purchased from Clinic funds or from grant funds, must be registered in the Unit information assets inventory.
4. All portable computing devices used in the UF HSC information and computing environment, regardless of ownership, must be approved by the Unit ISM, prior to enabling network connection.
5. All portable computing devices and media used by an HSC workforce member who has access to UF HSC or Shands Restricted information, must meet or exceed the security requirements of Standard TS0010 Portable Computing Device Security before being used.
6. UF HSC Units must provide resources necessary to secure Unit issued portable computing devices and media according to Standard TS0010 Portable Computing Device Security.
7. If resources necessary to secure *privately* owned portable computing devices and media according to Standard TS0010 Portable Computing Device Security are not provided by the Unit, the user is responsible for providing them.
8. The user of a portable computing device or media used to store, transmit, or process Restricted information is responsible for any misuse of the information by persons to whom they have given access to the device or media.
9. The user of a portable computing device or media used to store, transmit, or process Restricted information, must prevent use of the portable computing device or media by any unauthorized persons.
10. Should a portable computing device or media containing Restricted information become lost or stolen, the user must report the incident to their Unit ISM or the HSC Incident Response Team (HSCIRT@ufl.edu or 352 273-4478) within 24 hours of noticing it missing.
11. Users who fail to obtain necessary authorization, approval, who fail to apply required safeguards, or who fail to report a lost or stolen device or media containing Restricted information are subject to disciplinary measures up to and including termination.