Standard: TS0010.02	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: 2/2007

Purpose:

To establish a security standard for portable computing devices and media to preserve the confidentiality, integrity, and availability of Restricted information.

Reference:

SPICE Policy TS0010 Portable Computing Device Security
SPICE Standard TS0005.02 User Account and Password Management
SPICE Policy PS0003 Device and Media Controls
SPICE Standard PS0003.02 Device and Media Controls
Gatorlink Password Management Policy, http://www.it.ufl.edu/policies/passwords.html

Standards:

1. Unit authorization to remove Restricted information from the premises on portable computing devices or media must be expressly written in script or electronic format. Verbal authorizations are not acceptable. To reduce the volume of patient care related authorization requests, Units may place the following statement in local policy and procedure documentation to pre-authorize care givers for continuity of care:

   *Faculty and staff in UF care giver roles are authorized to have the **minimum necessary** electronic PHI on portable computing devices for purposes of continuity of care. The portable device and the PHI must meet or exceed security requirements of SPICE Policy and Standard TS0010 Portable Computer Device and Media Security. All other purposes (i.e. research, academic) and all other Unit roles must be authorized by <name of Dean, Directory, Dept Chair or Delegate> on a case by case basis. It is the user's responsibility to obtain the authorization.*

2. Unit information asset inventory records pertaining to portable computing devices must minimally include manufacturer and model of the device, a unique identifier of the device, user contact information, and classification of information stored.
3. Restricted information stored on a portable computing device or media must be limited to the minimum necessary to accomplish the purpose for which it was authorized.
4. The following safeguards must be applied to a portable computing device or media if the assigned user has been granted access to Restricted information:

a. The portable computing device and media must be configured to require a strong password of its user and administrator, consistent with or exceeding UF gatorlink password strength rules. Passwords must be maintained according to SPICE Standard TS0003 User Account and Password Management.
b. The portable computing device must be configured with an inactivity timeout requiring re-authentication, or an inactivity automatic logoff.
c. The portable computing device or media must be configured to encrypt all locations where Restricted data is likely to be stored. For laptops and tablet PCs, whole disk encryption must be deployed. The encryption pass phrase or encryption key must also meet or exceed the UF gatorlink password strength rules, and be kept secret. Where practicable, the key or pass phrase must be registered with a key management and recovery service approved by the Unit ISM.
d. The Restricted data must be protected by encryption during data transmission over any wireless network and any non-University wired network.
e. The portable computing device must be secured with a theft deterrent device such as a cable security kit, when the device needs to be operational and unattended.
f. The portable computing device and media must be stored under lock and controlled key when unattended and not in use.
g. The portable computing device must have a durable physical or electronic label affixed with the owners name and contact information for expedient return in the event that a lost device is found by an honest person.

5. Encryption must be included in the initial purchase of any new UF HSC portable computing device and media, regardless of intended use.
6. Restricted information stored on a portable computing device and media must be backed up to a secure server so the UF HSC can be compliant with Florida statutes on notification, should the device or media become stolen or lost.
7. Users must ensure that any authoritative copy of information needed for UF HSC business stored on portable computing devices and media is backed up to a secure server.
8. Restricted information stored on portable computing devices and media must be securely erased or destroyed as soon as the device is taken out of production or retrieved from the user to be repurposed.