UF UNIVERSITY of FLORIDA
Information Technology

POLICY

Policy: TS0012	Category: Technical Security	Version Date: 2/15/2017
Title: Computer Security Policy		Effective Date: 2/22/2017
Originating Unit: Information Security Advisory Committee		Last Review: 2/15/2017
Review Resp: HIPAA Security Officer		Next Review: 2/15/2020

Purpose:

To establish minimum security requirements for computers to protect UF data and IT resources from reasonably anticipated threats and hazards. Many of the security controls identified in this policy apply to computers regardless of the classification of data (Restricted, Sensitive, Open) to which they provide access. Without the security controls set forth in this policy, any computer can acquire a computer virus or worm, or is susceptible to computer hacking. A compromised computer on our internal network then becomes an instrument for unauthorized access to or infection of other computers on our network that may be critical or may provide access to Restricted information.

Scope:

This policy applies to all servers, computing appliances, desktops, portables, peripherals etc. capable of executing computer code and becoming compromised, and that are used for HSC business, connected to the HSC network, or used to store, process or transmit UF electronic Protected Health Information.

References:

1. UF Healthcare Computer Security Standards:
    a. TS0012.02 UF Owned or Managed Computer Security Standard
    b. TS0012.04 Personally or Affiliate Owned Computer Security Standard
2. UF Mobile Computing and Storage Devices Policy
3. UF Risk Management Policy

Policy:

1. Users who *store* Restricted information on a personally or affiliate owned computer 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.
2. Unit Dean, Director or Department Chair authorization is not required to *access* HSC Restricted information on a personally or affiliate owned computer. However, software used to *access* Restricted information from a personally or affiliate owned computer must be reviewed and approved by the Unit ISM who must first confirm the software does not store or cache Restricted data, temporary or otherwise, on the end user's computer hard drive. Users must seek this approval prior to using the software to access UF Restricted information.
3. Personally or affiliate owned computers used by University affiliates, students, faculty and staff for HSC business must comply with security standard TS0012.04. It is the responsibility of the user with system administrative privileges on the computer to ensure the required security

controls are implemented and maintained.

4. University owned or managed computers used for HSC business must comply with security standard TS0012.02. It is the responsibility of the Unit ISM to ensure the required security controls are implemented and maintained on all computers he or she registers for network access.
5. Unit ISMs must ensure an up-to-date inventory is maintained of any UF owned or managed computers used in their Unit and any computers they have registered for use on the UF or UFHealth wired and wireless networks.
6. The Unit must perform a security evaluation on computers that will be used to store Restricted information, will be used to provide concurrent user access to Restricted information (i.e. server), or that reside in the Open network security zone.
   a. The recommendations generated from the security evaluation must be completed prior to use of the computer in production, prior to use by users and prior to interaction with Restricted information unless otherwise stated in the evaluation report.
   b. The Information Security Office may require or initiate security validation testing for the purpose of identifying vulnerabilities.
   c. Computers determined by the security evaluation process to present an unacceptable security risk to the HSC are prohibited from accessing or using the HSC network, and from interacting with HSC Restricted information.
7. The Unit ISM and/or Unit ISA, in concurrence with the Information Security Office, may at any time disconnect a computer from the UF or UFHealth network that has been verified to create an unacceptable security risk.
8. Failure to comply with this policy will be reported as an information security violation and may result in loss of network and system privileges for the computer and the individual violating the policy.