UNIVERSITY of FLORIDA

Standard

Standard: TS0012.02	Category: Technical Security	Version Date: 2/15/2017
Title: UF Owned or Managed Computer Security Standard		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 provide computer security standards that must be met to comply with TS00012 Computer Security Policy.

Scope:

This standard applies to all UF owned computers used for HSC business, connected to the HSC network, or any other computer used to store, process or transmit electronic Protected Health Information.

References:

1. UF Account Management Policy
2. UF Password Complexity Standard
3. Item #189 Access Control Records, State of Florida General Records Schedule GS1-SL.
4. UF Mobile Computing and Storage Devices Policy
5. TS0012.04 Non-UF Owned and Managed Computer Security Standard

Standard for UF Owned or Managed computers:

A. Computer inventory requirements:
   1. Make, model, mfg
   2. Unique identifier (asset tag or serial number)
   3. User if applicable
   4. Location in terms of IP or bldg & floor (with exception of mobile devices)
   5. System administrator or system administrator team
   6. Unit
   7. Recoverability Objective (as determined by the services it provides)
      a. 0-24 hours (critical)
      b. 0-72 hours (not critical)
      c. Two weeks (not critical)
      d. As resources are available (not critical)

B. Product Support - the publisher of the operating system (OS) must still be developing and distributing security patches for the version resident on the computer.

C. Support – computers will have a clearly defined system administrator or system administrator team whose responsibility is to ensure the protections in this standard are implemented and maintained.

D. Anti-Malware (AM) protection:
   1. Each networked computer will have anti-malware software installed.
   2. The detection engine and malware definition files of the anti-malware software will be configured to be automatically updated as supported by the anti-malware software provider.

E. Host based firewall protection
   1. Computers will have a host based firewall.
   2. The firewall will be configured to allow only the ports and services needed to function for UF business purposes.

F. Inactivity timeout
   1. Computers will be configured with an inactivity timeout requiring re-authentication to regain access to the host session. The inactivity timeout requirement is in addition to, not a substitute for, the requirement that the user manually lock the workstation when they walk away (i.e. Ctrl-Alt-Del >> Lock Computer for windows).
   2. The inactivity timeout value of the computer will be established commensurate with risk to information assets accessible through the computer, taking into consideration the security afforded to the physical environment in which the computer operates. In the absence of a risk based timeout value determination by the Unit, the following guidelines should be used on computers used to access Restricted information:
      a. Private office setting where the office has a locking door which is kept closed and locked during business hours when unattended: not to exceed 30 minutes
      b. Semi-private work area that is not or cannot be locked during business hours when unattended and is exposed to other faculty/staff passersby but not the general public; reception desk, office, cubicle: not to exceed 15 minutes
      c. Public area where the workstation is not always attended and is exposed to general public passersby:
         i Clinic hallway - not to exceed 5 minutes
         ii Reception desk workstation - not to exceed 5 minutes
         iii Exam room where patient is left alone with the workstation - not to exceed 5 minutes
      d. Operating Rooms, Intensive Care Units or Emergency Room - discuss with Privacy/Security offices; this will be situational due to the fact that there are workstations performing different functions in these critical care areas.

G. Computer account management
   1. All people, entities, and processes (scripts, applications) with computer accounts will be uniquely identified, with the following exceptions:
      a. Accounts on single purpose computers such as data collection instruments and appliances that have no interaction with Restricted data, and no Internet connection do not require unique identification.
      b. Accounts on computers do not require unique identification if all other applications, data, and networks (including the Internet) accessible by the computer individually require unique identification to access.

2. All computer accounts will be established using the least privileged principle; privileges will be limited to that which is necessary for the person, entity or process to carry out their functions on the computer.
3. The authentication process of the computer will be protected from brute force (automated robotic login attempts) attacks such as suspending an account that is attempting and failing to logon repeatedly in a short period of time.
4. Password strength requirements for access to a computer will meet or exceed those specified in the UF Password Complexity Standard.

H. Operating system (OS) security patch management must be applied to computers. Either of the following methods are acceptable:
   1. System administrators subscribe to alerts from OS publishers for notification of new security patches, test the available patches in a non-production environment, and apply the patches as soon as they can be safely applied.
   2. System administrators configure computers to automatically detect, download and install security patches per OS publisher recommendations.

I. Network security zone assignment – Computers are afforded certain protections by the network depending upon the network security zone in which they are placed. Unit ISMs are responsible for assignment of computers to the appropriate network security zone based on *business needs* of computers and users to interact with main campus computers and Internet resources:
   1. Closed Zone usage –computers requiring and providing no services outside of Shands and the HSC; i.e. clinical instruments, database servers, printers.
   2. Protected Zone usage – computers needing access to the Internet but should not have uninitiated access 'from' the Internet; i.e. end user workstations.
   3. Campus Zone usage – computers that provide a service to users on main campus but not to the general public of Internet users. Main campus departments such as BME, PPD, HR, OGC etc. with sites in the HSC might use the Campus Zone for communication with their main campus colleagues.
   4. Open Zone usage – limited to servers that provide a service for Internet users

J. Computer activity logging – System administrators must configure computer activity logging as follows:
   1. Computers must minimally log identity and date/time stamps of the following security events:
      a. Access or logins and logouts to the computer
      b. User creations, privilege escalations and group membership changes that affect user permissions
      c. software installations/de-installations
      d. start-up/shutdown
   2. Logs for computers provisioning services to multiple users over the HSC network (i.e. servers, workstations configured as servers) must be retained for a minimum of 12 months (per State of Florida General Records Schedule; see references) and a maximum

of 14 months. Other computers must retain logs for a minimum of 30 days and a maximum of 90 days.

3. Logs from computers in the Open Zone must be stored in a separate logging server. Logs from computers in the Open Zone must be monitored and alerts sent to the system administrator for suspected intrusion or compromise events.

K. Additional Safeguards for Critical computers:
   1. Critical computers will be acquired from known credible sources with hardware maintenance support offerings. There will be a hardware support plan in place commensurate with the Criticality of the computer.
   2. System administrators will maintain and follow a documented configuration management process that minimally includes the following:
      a. System administrators will maintain a backup copy of the configuration in a secure area. The backup will be performed each time the configuration of the critical host changes.
      b. System administrators will implement a mechanism to detect and alert on unauthorized changes to the configuration of a critical computer.
      c. System administrators will maintain and follow a documented change management process when making configuration changes to a critical computer. Change management process for critical computers will minimally include:
         i Change authorization
         ii Communication/scheduling with appropriate stakeholders
         iii Pre-planned back out process
         iv Change log with description of the change, actual date/time of the change and system administrator applying the change.

L. Vulnerability scanning and remediation of networked computers will be done on the following schedule:
   1. System administrator will scan and remediate newly built or rebuilt computers, after configuration and prior to production network connectivity. In the case of a mass deployed computer image, scanning one computer is acceptable; however, remediation must occur on all installed instances of the image. Scans can be requested from the Information Security Office.
   2. System administrator will scan and remediate computers after a change to network software running on the computer or after installation of any service. Scans can be requested from the Information Security Office.
   3. All computers will be scanned by the UF Information Security Office at least every 30 days. Remediation of critical vulnerabilities must be completed by the system administrator within 10 business days of notification, or within 5 days for computers in the Open Zone.