Standard: TS0012.04	Category: Technical Security	Version Date: 10/28/2008
Title: Personally or Affiliate Owned Computer Security Standard		Effective Date: April 5, 2009
Originating Unit: Security Program for the Information and Computing Environment Project		Last Review: 10/28/2008
Review Resp: SPICE Program		Next Review: 10/2009

Purpose:

To provide computer security standards that must be met to comply with TS0012 Computer Security Policy.

Scope:

This standard applies to all personally or affiliate owned computers used for HSC business or connected to the HSC network.

References:

1. University of Florida software licensing site; anti-virus software: http://software.ufl.edu.
2. TS0005 User Account and Password Management Policy: https://security.health.ufl.edu/policies/#ts0005
3. GatorLink password strength: http://www.bridges.ufl.edu/gatorlink/tips.html
4. TS0012.02 UF Owned and Managed Computer Security Standard: https://security.health.ufl.edu/policies/#ts0012
5. TS0010.02 Portable Device and Removable Media Security Standard: https://security.health.ufl.edu/policies/#ts0010

Definitions

https://security.health.ufl.edu/policies/#gp0003

Standard for Personally or Affiliate Owned Computers

A. Restricted information *storage* authorization:
   1. Unit authorization to *store* Restricted information on a personally or affiliate owned computer must be expressly written in script or electronic format. Verbal authorizations are not acceptable.
   2. This authorization must have an expiration period commensurate with the project's duration and may not exceed 24 months. If the project will extend beyond 24 months, the authorization must be renewed bi-annually.
   3. To assist the Dean, Director or Department Chair in making an informed authorization decision, Units may require users to attest to the security of their personally or affiliate owned computer prior to receiving authorization to store. See Exhibit A for a computer security attestation form.
      a. The form should be completed to the satisfaction of the Unit ISA or ISM.
      b. The Unit should establish a period in which the attestation expires and is revisited by the user.

B. Approval of software that *accesses* Restricted information: Any software the user wishes to use to *access* Restricted data from a personally or affiliate owned computer must be reviewed and approved by the Unit ISM*.
   1. The store/cache feature on software providing access to Restricted data must be disabled.
   2. If the software does not allow the store/caching feature to be disabled, the user must seek authorization to store Restricted data off premises prior to using the software on a personally or affiliate owned computer (see A. above.)

3. Software found to provide user access to Restricted data without storing/caching the data on the end user's computer hard drive does not require approval from the Dean, Director or Department Chair.
4. To streamline this review and approval process, Unit ISMs must publish on their departmental web site, the list of software they have approved for Restricted data access from personally or affiliate owned computers.

C. Criticality – Personally or affiliate owned computers may not be used to provision services critical to an HSC department.
D. Security controls - Personally and affiliate owned computers will be permitted on the HSC network under the following conditions:
   1. The user can successfully authenticate using gatorlink credentials
   2. The computer can pass a security posture assessment test for:
      a. Up to date operating system security patches
      b. Up to date antivirus signature files
      c. Computer based firewall
E. Network access – Network services provided to personally and affiliate owned computers will be limited to Internet access and University computing resources that are available to the general public. Personally and affiliate owned computers requiring additional network access to conduct HSC business must meet Unit security requirements for managed HSC computers and must be approved by the Unit ISM.

* Note: Many applications store data on the hard drive of the computer without user intervention or knowledge. Examples include Microsoft Outlook and Internet Explorer. This application design exists primarily 1) to improve speed with which the application responds to users' request for data and 2) many applications in production today were designed before security principles were required. The intention of this application approval process is to test and ensure the application does not store data on the hard drive of the end user computer without user intervention.

Exhibit A – Personally or Affiliate Owned Computer Security Attestation

Security Control	Yes	No	Comment
1. The HSC or Affiliate User has completed the UF HSC HIPAA & Privacy Training and has signed the UF HSC Confidentiality Statement within the past 12 months. http://privacy.health.ufl.edu/	☐	☐	
2. All passwords, user and administrative, that enable access to the computer are strong (at least 8 characters, contains at least 1 capital letter, 1 lower case letter, 1 number, and 1 special character)	☐	☐	
3. All users of the computer have their own unique and separate accounts and Restricted data stored by the HSC or Affiliate user cannot be accessed by other users of the computer.	☐	☐	
4. The Guest account on the computer is disabled.	☐	☐	
5. Administrator type accounts on the computer are only used when system administration duties need to be performed and not during regular use. User type accounts are used during regular use.	☐	☐	
6. Data stored on the hard drive of a laptop, portable, tablet type computer are protected by whole (full) disk encryption.	☐	☐	
7. If the User stores UF Restricted information on the computer, the data are stored in a database or file folders that are protected by a strong password.			
8. If the HSC or Affiliate User uses a technical support person, the HSC or Affiliate User does not permit the technical support person to access the UF Restricted information on the computer while carrying out technical support duties.	☐	☐	
9. The computer has a firewall turned on that does not permit uninitiated access to it from the Internet except automatic anti-virus updates and automatic operating system patches.	☐	☐	
10. The computer has anti-malware software controls installed, the anti-malware software is activated, and its signature or 'dat' files are on an automated update schedule that does not exceed 1 week.	☐	☐	
11. The computer is on an automated operating system patch schedule that does not exceed 1 month.	☐	☐	
12. The computer will lock after a period of inactivity not to exceed 30 minutes. The HSC or Affiliate User must enter the strong password to re-gain entry.	☐	☐	

Exhibit A – Personally or Affiliate Owned Computer Security Attestation

Security Control	Yes	No	Comment
13. The HSC or Affiliate User does not retrieve or send UF Restricted information over a network unless the files are protected by encryption (i.e. encrypt the files before retrieving/sending or transmit the information through an encrypted tunnel such as a VPN or SSL.)	☐	☐	
14. The HSC or Affiliate User has not installed and does not use a P2P file sharing programs such as LimeWire, BearShare, Kazaa, eDonkey, etc. on the computer to acquire music, videos and software games since such software shares folders on the Internet that the User had not intended.			
15. HSC or Affiliate User will not copy UF Restricted information to removable media such as CD, DVD, flash memory stick, removable hard drive, etc. without encryption protection.	☐	☐	
16. The HSC or Affiliate User will securely erase the UF Restricted information, or degauss or destroy the computer hard drive at the conclusion of the contract or when the data are no longer needed to be stored on the HSC or Affiliate User's computer, whichever comes first. The HSC or Affiliate User will provide a letter to the Unit ISM certifying the data destruction action and method used.	☐	☐	

The answers provided to the statements above have been researched and validated as they pertain to the computer on which I will store UF Restricted information.

HSC or Affiliate User's Printed Name and Signature _____ Signature Date _____ Expiration Date _____

☐ Approved ☐ Not Approved ISA/ISM Signature _____ Date _____

This approval should not be construed as a double check or a validation of the security controls the user claims to have implemented in the checklist above; it assumes the security control responses to be true. This approval pertains to residual risk of the HSC or Affiliate user storing UF Restricted data on the computer with the described security controls to which the computer user attested to above.

Conditions of Approval (unmet security requirements to be resolved, additional controls for unusual circumstances, etc.):

Exhibit A – Personally or Affiliate Owned Computer Security Attestation