Title: Workstation Security Standard

Scope: This standard is applicable to all VCU School of Medicine personnel.

Approval Date: July 1, 2010

Effective Date: July 1, 2010

Compliance Date: January 1, 2011

Authority: VCU School of Medicine Information Security Manager

Review Frequency: Annually, or as needed

Revision History:

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Revision Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>March 11, 2010</td>
<td>Draft approved by IT Audit Resolution Committee</td>
</tr>
<tr>
<td>1.1</td>
<td>June 14, 2010</td>
<td>Modifications related to changes in data classification guidelines</td>
</tr>
<tr>
<td>1.2</td>
<td>June 29, 2010</td>
<td>Modifications related to ITARC members feedback</td>
</tr>
</tbody>
</table>
I. PURPOSE
The Workstation Security Standard addresses the security and configuration
of VCU or VCUHS owned computer workstations that are used by VCU
School of Medicine employees or affiliated personnel.

II. POLICY
Various computer workstations can currently be used to access and store
business information through electronic mail and network or local file storage.
The information accessed on these devices may be sensitive in nature, and the
confidentiality, integrity and security for the sensitive data must be ensured in
order to comply with any legal, regulatory and administrative requirements.
This document states the minimum security standards with regard to the
configuration and use of computer workstations for business purposes in the
VCU School of Medicine.

III. DEFINITIONS
Administrative Rights – The highest level of permission that is granted to a
computer user. This level of permission allows the user to install any software,
hardware, and change security control and configuration settings on a
computer.

Authoritative Unit Head – A VCU or VCUHS employee who has the
ultimate decision making authority within a business unit or a department in
the VCU School of Medicine.

Authorized User – An individual who has been granted access to specific data
in order to perform his / her assigned duties in the VCU School of Medicine.

Autorun Feature – A feature on certain computer operating systems that
allows the automatic execution of programs stored on an external storage
media.

Centrally Managed File Server – A server that is located in a geographically
dispersed and professionally managed data center. This server is designed to
manage the storage and access control to data that is logically stored on the
server.

Confidential and Protected Data – Confidential and Protected data are
considered the most sensitive, and must be protected with the highest security
standards. These data are protected specifically by federal or state law and
regulations (e.g. HIPAA, FERPA.) Loss of confidential and protected data
can result in long term loss of funding, ranking and reputation for the school,
as well as possible legal actions against the University, School, or the data
owner. Confidential and protected data are a subset of sensitive data;
therefore, all confidential and protected data are also classified as sensitive.
Examples include student or employee SSN, date of birth, Electronic
Protected Health Information (E PHI), and student grades. Refer to the "School of Medicine Data Classification Guidelines" for authoritative definitions.

**Data Owner** – The Data Owner is the VCU or VCUHS employee responsible for the policy and practice decisions regarding data, and is responsible for evaluating and classifying sensitivity of the data; defining protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs; communicating data protection requirements to the System Owner; defining requirements for access to the data.

**Desktop Management System** – A Desktop Management System is an enterprise system used to manage multiple computers within an organization. The management features typically include vulnerability scanning, software patch management, asset management, computer imaging, software distribution, and license management. Examples include LANDesk, Microsoft Systems Management Server (SMS), and KACE.

**Guest Account** – On a computer, a guest account is a user login account with limited rights, but does not require a password.

**IT System** - An IT System is a combination of people, hardware (computer workstation, mobile device, removable storage media, server), software, communication devices, network and data resources that processes (can be storing, retrieving, transforming information) data and information for a specific purpose.

**Network Authentication Account** – A network authentication account allows the user of a computer workstation to logon to a specific system and receive access to data stored on the network that is authorized to that particular user. Examples of a network authentication account include Novell login accounts, Microsoft Active Directory login accounts, and web application accounts

**Non-sensitive Business Data** - Non-sensitive business data are non-personal data that are not necessarily proprietary to an institution. The protection of these data are neither regulated nor controlled by law or contractual obligations, as the protection of the data is at the discretion of the data owner. If lost or illegitimately modified, these data will generate no negative impacts to individual business units or the institution as a whole. Refer to the "School of Medicine Data Classification Guidelines" for authoritative definitions.

**OS Firewall** – A software firewall application built into the operating system to allow filtering of incoming and / or outgoing network traffic for that computer system.
Real-time Virus Protection – The real-time virus protection feature of an antivirus system that allows it to automatically scan files as they are being written to the disk. The VCU or VCUHS supplied antivirus systems have this feature enabled by default.

Principle of Least Privilege – This principle requires that each user in a system be granted the most restrictive set of privileges (or lowest clearance) needed for the performance of authorized tasks.

Publicly Accessible Area – Physical spaces that are not located behind locked doors and can be accessed freely by any individual without any form of identification or key. Examples include reception area in a clinic, an unlocked classroom, or a hallway in an unrestricted building.

Sensitive Data – Data that are proprietary to an institution, where if lost or illegitimately modified, can cause negative impact to the individual units or the institution as a whole. Examples include employee performance evaluations, faculty salary or contract information, and proprietary research data.

System Administrator – An analyst, engineer, or consultant who implements, manages, and/or operates an IT system and manages the data that is stored on that system at the direction of the System Owner and Data Owner. The System Administrator implements security controls and other requirements of SOM information security program on an IT system for which he or she has been assigned responsibility.

System Owner – A VCU or VCUHS employee who is responsible to authorize or deny access to IT system to system users. The system owners are directly responsible for the physical and logical security of the computer workstations that are under their control.

System User – A VCU or VCUHS personnel or affiliate who is authorized by the System Owner to have access to a VCU School of Medicine computer workstation. A system user can consist of faculty members, graduate students, post doctoral associates, staff members, vendors, external organization users, and any other affiliates who have access to a VCU School of Medicine computer workstation.

Wake-on-LAN – A feature on certain computers that allows the computer to be powered on remotely by a user or administrator.

IV. RESPONSIBILITIES
All VCU School of Medicine system users who use computer workstations to access, process and store business data, are responsible for following the security requirements set forth in this standard.

The system owner is directly responsible for authorizing, reviewing and revoking access to computer workstations to any VCU or VCUHS personnel. Further, the system owner is also directly responsible for the logical and physical security of the computer workstations.

The system administrator is directly responsible for configuring computer workstations according to security standards set forth in this standard, granting and revoking access to computer workstations and data at the direction of the System Owner and Data Owner.

The VCU School of Medicine Information Security Manager is responsible for reviewing and auditing this standard annually.

V. LOGICAL ACCESS CONTROL

A. All VCU or VCUHS owned computer workstations used by the VCU School of Medicine must have a clearly defined system owner.

B. Access to computer workstations must be authorized by the system owner or a designee.

C. The system owner or the designee must notify the appropriate system administrator(s) within 24 hours of personnel transfer, termination, or suspension. The system administrator must then revoke the employee’s physical and logical access to computer systems within 3 business days of the initial notification.

D. Access to computer workstations must follow the principle of least privilege.

E. Unique user names and passwords must be assigned to individuals to access computer workstation(s).

F. All user accounts on computer workstations must have passwords that are at least 7 characters long, and contain at least one uppercase character, one lowercase character, and one numeric character. Passwords for all user accounts must be changed at least once per year.

G. Passwords to all accounts cannot be documented and stored in plain text. Digital password management software such as Keepass can be used to manage and store passwords securely.
H. Computer workstations must use password enabled screen savers to automatically lock out or log off (if supported by Operating System) a session following no longer than 30 minutes of inactivity.

VI. PHYSICAL ACCESS CONTROL

A. If applicable, computer workstations that have access to sensitive data should be placed behind locked doors. Access to these locations should be restricted to authorized users of the computer workstation.

B. Computer workstations with locally stored sensitive data must be placed behind locked doors. Access to these locations must be restricted to authorized users of the computer workstation.

C. Publicly accessible computer workstations, regardless of sensitivity must be physically secured with locking mechanisms such as pad lock or cable lock.

D. Mobile computer workstations such as laptops must never be left unattended in a publicly accessible area. These workstations should be secured with cable locks if possible.

E. After-hours access to the VCU School of Medicine facilities must require appropriate monitoring and auditing.

VII. DEVICE CONFIGURATION AND SECURITY MANAGEMENT

The following device configuration and security requirements apply to all computer workstations, except research equipment workstations used to access and/or store sensitive data:

A. Usage of shared network authentication accounts on computer workstations is strictly prohibited. All users of a computer workstation must have their own dedicated network authentication accounts.

B. Password requirement and complexity filters must be enabled on all computer workstations.

C. All computer workstations connected to the VCU or VCUHS network must use an Operating System that is currently supported by the vendor.
D. Guest accounts must not be enabled or used on any computer workstations.

E. The auto-run feature must be disabled on all removable media on all computer workstations.

F. Automatic or centrally managed Operating System update must be enabled for all computer workstations.

G. A desktop management system must be used to centrally monitor and patch third-party software security vulnerabilities on all computer workstations.

H. Any Wake-on-LAN or similar remote power management features must be disabled if it is not needed.

I. University or Health Systems approved antivirus software must be installed and activated on all computer workstations. The antivirus software must have up-to-date virus definitions and must be enabled for real-time virus protection.

J. At a minimum, an OS firewall must be installed and activated on all computer workstations attached to the VCU or VCUHS network.

K. Local administrative rights, (or the equivalent on non-Microsoft Windows-based IT systems) on computer workstations must be restricted. Administrative rights on computer workstations that contain or have access to sensitive data must be authorized by authoritative unit head.

L. All computer workstations are intended to be used for business purposes; a clearly documented computer usage policy must be defined by unit head and communicated to all system users.

VIII. DATA STORAGE AND TRANSMISSION

A. Any sensitive data stored on removable storage devices must be encrypted with an industry approved encryption algorithm.

B. No sensitive data can be stored locally on the computer workstations unless the data is encrypted and there is a written exception approved by the appropriate Information Security Officer. Otherwise, all sensitive data must be stored on centrally managed file servers.

C. All off-site remote connections and sensitive data transmission to and from the computer workstations must utilize means of encryption.
Encryption is required for session initiation and all transmission of sensitive data.

IX. REPORTING LOSS AND THEFT OF EQUIPMENT OR DATA

In the event a computer workstation is lost or stolen, the theft or loss must be reported immediately to the VCU police at 828-1196. In the event that sensitive data is suspected lost or stolen, the theft or loss must be reported immediately to the VCU information security office at 828 – 1105 or VCUHS information security office at 628 – 1144.

X. DISPOSAL OF DEVICE

A. All data on computer workstations must be securely removed prior to disposal. The data removal process must be in compliance with the DOD 5220.22-M standards, where no data recovery will be possible from the computer workstation.

B. Backups of sensitive data that are no longer needed must also be securely destroyed according to the DOD 5220.22-M standards.

XI. EXCEPTIONS

Exception requests to this standard must be filed with, and submitted to, VCU School of Medicine Information Security Manager. Any exception request should use the exception request form attached in appendix A.

XII. COMPLIANCE

Compliance with this Workstation Security standard is the responsibility of all personnel who use computer workstations to access, process and store sensitive VCU School of Medicine data. This document establishes standards for these personnel’s actions in recognition of the fact that these personnel are provided unique system and data access, and that non-compliance to this standard will be enforced through sanctions commensurate with the level of infraction. Administrative actions due to failure to follow this standard may range from a verbal or written report, temporary revocation of system and data access, termination of employment, to legal proceedings against the personnel depending on the severity of the violation. All personnel who have access to School of Medicine data are expected to read, understand and agree to the responsibilities defined in this standard and any published revisions of this standard.

XIII. REFERENCES

A. VCU Information Security Standard section 4: IT Systems Security
B. VCU Information Security Standard section 5: Logical Access Control
D. VCU Affiliated Covered Entity ACE-0013: Workstation Security
E. NIST Special Publication 800-68: Guide to Securing Microsoft Windows XP Systems for IT Professionals
### Appendix A. VCU SOM Information Security Standards Exception Request Form

<table>
<thead>
<tr>
<th>Requestor:</th>
<th>Unit Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Authoritative Unit Head:</th>
<th>Contact phone:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Requirement to which an exception is requested (Section, Item #)</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Provide the business or technical justification for exception:

2. Describe the scope, including quantification and requested duration (not to exceed 1 year):

3. Describe all associated risks, including the sensitivity and criticality of hardware or data involved in exception:

4. Identify the compensating controls to mitigate the risks:

5. Identify any unmitigated risks:

6. When will compliance with policy be achieved?

By submitting this form, the Authoritative Unit Head acknowledges that he or she has evaluated the business issues associated with this request and accepts any and all associated risks as being reasonable under the circumstances.

Authoritative Unit Head Signature: ________________________________

Date: ________________________________

<table>
<thead>
<tr>
<th>SOM Information Security Manager Use Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval:</td>
</tr>
<tr>
<td>__ Approved    __ Denied</td>
</tr>
<tr>
<td>__ VCU/VCUHS Approval Required</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Signature: ______________________________</th>
<th>Date: ______________________________</th>
</tr>
</thead>
</table>
Completed exception forms must be submitted to SOM Information Security Manager by e-mail, somsecurity@vcu.edu

Contact information:

**SOM Information Security Manager:** 827-9907 Phone  
**VCU Information Security Officer:** 828 – 1015 Phone  
**VCUHS Information Security Officer:** 628 – 1144 Phone