Title: Research Equipment 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>December 3, 2009</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 Research Equipment Workstation Security Standard addresses the security and configuration of computers integrated with or attached to proprietary research equipment in the VCU School of Medicine, regardless of ownership of the device.

II. **POLICY**

Various types of proprietary research equipment are attached to computer workstations to store, manage and access research data either stored locally or stored in centrally managed server storage. Due to the proprietary nature of research equipment and related software, it is not always possible to keep the attached workstation up-to-date and compatible with current versions of operating system either because of lack of vendor support or the costs involved. These workstations with outdated operating systems pose a significant risk to the enterprise network. The research equipment is often deemed critical for research projects and therefore discontinuing the use of such equipment is not always a feasible option. Consequently special care must be taken to protect these workstations to minimize the security risk. This document provides the minimum security standards for computers attached to proprietary research equipment. All users of research workstation equipment are expected to abide by this standard.

III. **DEFINITIONS**

**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.

**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 (EPHI), 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.

**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.

**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.

**Removable Storage Media** - Device or media that is readable and/or writeable by a system user and is able to be moved from computer to computer without physical modification to the computer. This includes flash memory devices such as thumb drives, cameras, MP3 players and memory cards; removable hard drives (including hard drive-based MP3 players); optical disks such as CD and DVD disks; floppy disks and any commercial music and software disks.

**Research Equipment Owner** – The VCU or VCUHS employee who can authorize access to research equipment workstations, and is directly responsible for providing this access.
**Research Equipment Workstation** – Dedicated standalone or networked computer(s) or workstation(s) that are connected to research equipment, and are designed to operate that equipment. A research equipment workstation may also access, process and store the data to and from the research equipment.

**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.

### IV. RESPONSIBILITIES

All VCU School of Medicine faculty, graduate students, post doctoral associates, and staff who use or manage research equipment workstations to access, process and store research data (sensitive or non-sensitive), are responsible for following the security requirements set forth in this standard.

The data owner of sensitive research data is directly responsible for the confidentiality, integrity and security of the data stored, processed, and/or transmitted via the research equipment workstations.

Research equipment owner is directly responsible for authorizing and providing access of the research equipment to any VCU or VCUHS employee. Further, the research equipment owner is also directly responsible for the logical and physical security of the research equipment and the research equipment workstation.

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

### V. LOGICAL ACCESS CONTROL

A. Each research equipment workstation must have a clearly defined research equipment owner.

B. Access to research equipment workstations must be authorized by the research equipment owner or a designee.

C. Access to research equipment workstations must follow the principle of least privilege.

D. If possible, unique user names and passwords should be assigned to all users of research equipment workstations. No shared network
authentication accounts are permitted under any circumstances.

E. All user accounts on the research equipment 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.

F. All research equipment workstations must only be used for intended research purposes, any unneeded software or features must be removed or disabled from the research equipment, and a usage policy must be defined and clearly communicated to all users of the equipment.

G. Research equipment owners or a designee should stay in contact with the research equipment vendor and keep abreast of any software, security or operating system upgrades available for their research equipment.

H. Passwords to all accounts must be documented and stored securely; no passwords can be stored in plain text. Digital password management software such as Keepass can be used to manage and store passwords securely.

I. Research equipment workstations must use password enabled screensavers to automatically lock out a session following 30 minutes of inactivity.

VI. PHYSICAL ACCESS CONTROL

A. If possible, research equipment workstations should be placed behind locked doors. Access to these locations must be restricted to authorized users of the research equipment.

B. Publicly accessible research equipment workstations must be physically secured with locking mechanisms such as pad lock or cable lock.

C. Laptops used as research equipment workstations must be physically secured with locking mechanisms such as pad lock or cable lock.

D. After-hours access to the research facility must require appropriate monitoring and auditing.

VII. DEVICE CONFIGURATION AND SECURITY MANAGEMENT
The following device configuration and security recommendations apply to all research equipment workstations used to access and/or store sensitive data:

A. If applicable, avoid the usage of shared user accounts on research equipment workstations. All users of a research equipment workstation should have their own dedicated accounts.

B. If applicable, password requirement and complexity filters must be enabled on the research equipment workstation.

C. All research equipment workstations connected to the VCU or VCUHS network must use a vendor supported Operating System and all vendor-approved security patches must be installed in a timely manner.

D. Guest accounts must not be enabled and used on any research equipment workstations.

E. The autorun feature must be disabled for all research equipment workstations.

F. The research equipment workstations should be disconnected from the network, if network access is not needed.

G. All unneeded peripheral connections and ports must be disabled on research equipment workstations.

H. At a minimum, antivirus software must be installed and activated on research equipment workstations.

I. If applicable, research equipment workstations attached to the network should have an enabled firewall.

J. If applicable, local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, should be restricted on research equipment workstations.

VIII. DATA STORAGE AND TRANSMISSION

A. Any sensitive data stored on research equipment workstations and/or attached removable storage media must be encrypted with an industry approved encryption algorithm.

B. If possible, research equipment workstations should utilize centrally managed file servers for data storage. Any research equipment
workstation that stores data locally must have an appropriate backup infrastructure implemented, where the data captured by and stored on the research equipment workstation must be backed up on a daily basis.

C. All off-site remote connections and data transmission to and from the research equipment workstations that contain or have access to sensitive data 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 research equipment 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 research equipment 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 research equipment 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 Research Equipment Workstation Security standard is the responsibility of all personnel who use research equipment 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
   F. NIST Special Publication 800-18 Revision 1
## 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>Authoritative Unit Head:</td>
<td>Contact phone:</td>
</tr>
<tr>
<td>Requirement to which an exception is requested (Section, Item #)</td>
<td>Date:</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: ______________________________________________________________________

---

### SOM Information Security Manager Use Only

<table>
<thead>
<tr>
<th>Approval:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>__ Approved  __ Denied</td>
<td></td>
</tr>
<tr>
<td>__ VCU/VCUHS Approval Required</td>
<td></td>
</tr>
</tbody>
</table>

Signature: ______________________________ Date: ______________________________
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