Title: Physical 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

<table>
<thead>
<tr>
<th>Revision History:</th>
<th>Version</th>
<th>Date</th>
<th>Revision Issuance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>January 25, 2010</td>
<td>Draft approved by IT Audit Resolution Committee</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>June 14, 2010</td>
<td>Modifications related to changes in data classification guidelines</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>June 29, 2010</td>
<td>Modifications related to ITARC members feedback</td>
<td></td>
</tr>
</tbody>
</table>
I. PURPOSE
The Physical Security Standard addresses the security of physical facilities and locations that contain or have access to business data in the VCU School of Medicine.

II. POLICY
Various facilities within the VCU School of Medicine are currently used to conduct business operations. The data accessed from these locations 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 for these facilities in order to ensure the protection of resources including personnel, the facility in which they work, as well as the data, equipment, support systems and media. All VCU School of Medicine personnel are expected to abide by the requirements stated in this document.

III. DEFINITIONS

Assigned Facility – A VCU or VCUHS facility that is assigned to VCU or VCUHS employee(s) for business operation purposes.

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.

CCTV Systems – CCTV systems are also known as Closed-circuit television. It is the use of video cameras to transmit video images to a specific monitoring station. These systems are typically used for surveillance purposes.

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.

**Facility Owner** – The Facility Owner is the VCU or VCUHS employee who has the ability to grant or revoke physical access to VCU or VCUHS facilities at the direction of the data owner.

**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.

**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.

**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 personnel who use an assigned facility to access sensitive business data are responsible for following the security requirements set forth in this standard.

The data owner of sensitive data is directly responsible for the confidentiality, integrity and security of the sensitive data stored, processed, and/or transmitted to and from the assigned facility. Further, the data owner is also responsible for authorizing, reviewing and revoking the physical access to these data for VCU or VCUHS personnel.

The facility owner is directly responsible for authorizing, reviewing and revoking access to facilities that house VCU School of Medicine data to any VCU or VCUHS personnel at the direction of the data owner. Further, the facility owner is also directly responsible for the physical security of the facility.
The VCU School of Medicine Information Security Manager is responsible for reviewing and auditing this standard annually.

V. PHYSICAL ACCESS CONTROL

A. All VCU or VCUHS owned facilities that are used to store VCU School of Medicine data must have a clearly defined facility owner.

B. All sensitive data used for business related purposes in the VCU School of Medicine must have a clearly defined data owner.

C. Physical access to areas that physically or electronically store sensitive data must be authorized by the facility owner or a designee.

D. Physical access to areas that contain or have access to sensitive data must be authorized by the facility owner or a designee.

E. The data owner or the designee must collect any keys, key cards, or access tokens and notify the facility owner within 48 hours of an employee’s separation. The facility owner must then revoke the employee’s physical access to the facility within 3 days of the initial notification.

F. Physical access to areas that physically or electronically store sensitive data must be protected with a locking door.

G. Physical access to areas that contain confidential and protected data must be protected with a locking door.

H. Physical access to areas that contain confidential and protected data should require proper electronic or physical authentication prior to entry, and all access attempts must be logged.

I. Facilities used to physically or electronically store sensitive data must be locked when vacant. Public access to these areas is strictly prohibited.

J. Facilities that contain confidential and protected data must be locked when vacant. Public access to these areas is strictly prohibited.

VI. TECHNICAL AND ADMINISTRATIVE CONTROL

The following controls and recommendations apply to all VCU and VCUHS physical facilities that are used to store or have access to sensitive data:
A. Magnetic devices must not be placed on computers and electronic equipment in order to prevent damages to the equipment.

B. Computer grade surge suppressors must be used to protect business computers and workstations from power surges. The minimum energy absorption level for the surge protector must be rated at 1000 Joules or higher.

C. Workstations and equipment deemed as critical to business operations must be protected with uninterrupted power supply (UPS) systems, and physically located in facilities with adequate HVAC and humidity controls.

D. If applicable, facilities used to store confidential and protected data should utilize monitoring systems such as security cameras or CCTV systems.

E. Workstations and laptops with access to sensitive data and located in publicly accessible areas must be physically secured with cable locks or other locking mechanisms.

F. Workstations, laptops or other equipment that contain or have access to sensitive data must not be left unattended in publicly accessible areas.

VII. 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.

VIII. 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.

IX. COMPLIANCE

Compliance with this Physical Security standard is the responsibility of all VCU or VCUHS personnel who have access to sensitive VCU School of Medicine data. This 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.

X. REFERENCES
A. VCU Information Security Standard section 7: Physical Security
B. VCU Affiliated Covered Entity ACE-0014: Device and Media Controls
## 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:** ______________________________________________________________________

### SOM Information Security Manager Use Only

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

<table>
<thead>
<tr>
<th>Signature:</th>
<th>Date:</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</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