Title: Personnel 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></td>
<td>1.0</td>
<td>January 25, 2010</td>
<td>Draft approved by IT Audit Resolution Committee</td>
</tr>
<tr>
<td></td>
<td>1.1</td>
<td>June 14, 2010</td>
<td>Modifications related to changes in data classification guidelines</td>
</tr>
<tr>
<td></td>
<td>1.2</td>
<td>June 29, 2010</td>
<td>Modifications related to ITARC members feedback</td>
</tr>
<tr>
<td></td>
<td>1.3</td>
<td>July 9, 2010</td>
<td>Modifications related to further review by SOM senior management</td>
</tr>
</tbody>
</table>
I. **PURPOSE**
The Personnel Security Standard delineates the steps necessary to restrict access to IT systems and data to individuals who require such access as part of their job duties in the VCU School of Medicine.

II. **POLICY**
Access to various VCU School of Medicine business data are granted to employees, contractors, and affiliates of the VCU School of Medicine. In order to protect the confidentiality, integrity and availability of these data from abuse, misuse, and destruction by individuals, all access to VCU School of Medicine business data will require proper authentication and authorization.

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** – An authoritative unit head is a dean or equivalent administrative officer (e.g. associate vice president/provost). The authoritative unit head has responsibility for the security of data, systems and technology under their direct management control. Authoritative unit heads may receive advice and input from the CIO and ISO regarding security issues but ultimately must manage their data and technology in accordance with these standards commensurate with risk and cost.

**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.

**Business Function Owner** – A VCU or VCUHS employee who is directly responsible for providing the oversight for the performance and operations of a particular business function.

**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.

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.

IT System Users – IT system users are VCU and VCUHS employees, contractors, vendors, third-party providers, and any other authorized users of VCU School of Medicine IT systems, applications, telecommunication networks, data, and related resources.

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 illegally 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.

Sensitive Data – Data that are proprietary to an institution, where if lost or illegally 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.

Separation of Duties – Assignment of responsibilities such that no one individual or function has control of an entire process. It is a technique for maintaining and monitoring accountability and responsibility for IT systems and 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.

**IV. RESPONSIBILITIES**

Every member of VCU School of Medicine faculty, staff, contractors, and affiliates with access to sensitive business data is responsible for the confidentiality, integrity and security of the sensitive data stored, processed, and/or transmitted physically and electronically. All personnel with access to sensitive business data are required to follow the security requirements set forth in this standard.

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

**V. ACCESS DETERMINATION AND CONTROL**

A. Access to sensitive data in the VCU School of Medicine must be authorized and approved by the data owner.

B. Authorization of physical and logical access to sensitive IT systems and data and the facilities that houses them must follow the principle of least privilege.

C. Unique user names and passwords must be assigned to individuals for access to sensitive data stored in any VCU School of Medicine systems.

D. Individuals with access to sensitive data must keep his or her login information (combination of user IDs and passwords) confidential. Any sharing of individual user names or passwords is strictly prohibited.

E. The supervisors of IT system users must notify Human Resources department to conduct background investigations of IT system users commensurate with risks associated with access to sensitive IT systems or data as directed by VCU or VCUHS Human Resources. Existing users may be grandfathered under the policy and may not be required to have background investigations (Human Resources will coordinate the background investigation).
F. The supervisor of the IT system user must notify the appropriate system administrator(s) and IT support staff within 24 hours of personnel transfer, termination, or suspension due to disciplinary purposes. The system administrator(s) and IT staff must remove the personnel’s physical and logical access to systems under their control within 3 business days of the receipt of this notification.

G. Upon transfer or termination, the supervisor of the IT system user must ensure the return of VCU logical and physical assets that provide access to sensitive IT systems, data, and the facilities that house them.

H. The business function owner must establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of VCU prohibit a complete separation of duties, as directed by VCU Controller’s Office.

VI. INFORMATION SECURITY AWARENESS AND TRAINING

Information Security Awareness and Training requirements identify the steps necessary to provide all IT system users with awareness of information security requirements and of their responsibilities to protect information systems and data:

A. All IT systems users with access to sensitive data must complete an information security awareness training annually and certify their acceptance and understanding of the VCU and / or VCUHS ACE, and SOM information security standards.

B. All IT system users must receive information security training before (or as soon as practicable after) receiving access rights to VCU School of Medicine IT systems, and in order to maintain these access rights.

VII. ACCEPTABLE USE

Acceptable use requirements identify the steps necessary to define acceptable and permitted use of IT systems:

A. Any discussion and disclosure of sensitive data to individuals who are not authorized to receive these data is strictly prohibited.

B. All authorized users of sensitive data must accept, follow and certify their understanding of the VCU Acceptable Use Policy. The VCU Acceptable Use Policy can be found at http://www.ts.vcu.edu/policies/computeruse.html.

C. All IT System users must understand and accept the fact that VCU reserves the right to monitor, and access all data created, sent, received,
processed, or stored on VCU systems with a reasonable cause, at reasonable times, and after reasonable notice, except in the event of a bona fide emergency.

D. Administrative rights to IT systems that contain sensitive data must be authorized by authoritative unit head and restricted to authorized users only.

E. Copyrighted and licensed materials must be used in compliance with the applicable intellectual property and fair use laws and the *VCU Intellectual Properties Policy*. The *VCU Intellectual Properties Policy* can be found at [http://www.research.vcu.edu/p_and_g/ippolicy.htm](http://www.research.vcu.edu/p_and_g/ippolicy.htm)

F. Unencrypted transmission of confidential and protected data via electronic mail or other electronic transmission medium is strictly prohibited. All electronic transmission of confidential and protected data must be encrypted.

**VIII. 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.

**IX. 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.

**X. COMPLIANCE**

Compliance with this Personnel Security standard is the responsibility of all personnel who are authorized to access 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.
XI. REFERENCES
   A. VCU Information Security Standard section 6: Data protection
   B. VCU Affiliated Covered Entity ACE-0015: Access Controls
   C. VCU Affiliated Covered Entity ACE-0018: Person or Entity Identification
## Appendix A. VCU SOM Policy and Standard 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:</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 they have 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: ______________________________________________________________________

---

**VCU / VCUHS Information Security Officer (ISO) Use Only**

<table>
<thead>
<tr>
<th>Approval:</th>
<th>Comments:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approved</td>
<td>Denied:</td>
</tr>
<tr>
<td>__________</td>
<td>___________</td>
</tr>
</tbody>
</table>

CISO: ________________________________

Date: ________________________________
Completed exception forms must be submitted to VCU Information Security Office or VCUHS Information Security Office depending on the ownership of the data involved.

Contact information:

**VCU Information Security Officer**: 828 – 1015 Phone  
**VCUHS Information Security Officer**: 628 – 1144 Phone