The following summary of key security standards applies to all VCU School of Medicine systems that either contain or have access to VCU School of Medicine business data. For detailed information security standards, please visit the following web site: http://www.medschool.vcu.edu/technology/security/policies.html.

Definitions:

**Sensitive Data** – All data that are proprietary to VCU, VCUHS or VCU School of Medicine, 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. VCU School of Medicine classifies all business data generated, processed, and received by its employees as sensitive.

**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.

Key Security Standards:

| Workstation Security Standard | User must assign complex passwords for accounts used to access sensitive data. The complex password must be at least 7 characters in length, and contain at least one uppercase letter, one lowercase letter, and one numeric or special character. Shared network login accounts are prohibited. |
| Research Equipment Workstation Security Standard | These standards apply to all workstations attached to research equipment. |
| Handheld Mobile Device Security Standard | Handheld mobile computing devices are classified as SmartPhones, PDAs, and other palm sized computing and communication devices used for business purposes. |

| Physical Security Standard | Facility owner reserves the right to grant or revoke access to a facility. |
| Office doors and / or computers must be locked when a user steps away from the office. |
| Passwords must not be written and stored in areas without physical protection. |
| Documents containing sensitive information must be stored in a physically secure location. Examples include behind a locked door or in a locked drawer. |
| Cable locks must be used for business computer equipment located in a publicly accessible area. |
| Business workstations must be protected with computer grade surge protectors. |
- Servers deemed critical to business operations must be managed in the VCU or VCUHS data center.

**Personnel Security Standard**
- Unique user names and passwords must be assigned to individuals for access to sensitive data stored in any VCU School of Medicine systems.
- Individuals with access to sensitive data must keep his or her user IDs and passwords confidential. Any sharing of individual user names or passwords is strictly prohibited.
- All IT System users must complete an information security awareness training annually and certify their acceptance and understanding of the VCU and / or VCUHS ACE information security standards.
- 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 bonafide emergency.
- 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.

**Data Handling and Storage Standard**
- A data owner must be clearly defined for all business data that is produced, accessed and stored using VCU School of Medicine facilities and workstations.
- The data owner reserves all rights to the data, and is responsible for determining access controls, transmission, and data retention.
- All confidential and protected data must be stored on centrally managed network servers under all circumstances.
- Sensitive data must be stored on centrally managed network servers unless it is authorized by the Information Security Officer, backed up according to VCU or VCUHS standards, and encrypted with industry approved algorithms.
- All personnel must use individual and unique passwords to logon to any network systems.
- Users must not share their passwords with others.
- Passwords must not be stored, sent or received in clear text.
- Point to point encryption is required when confidential and protected data is accessed or transferred.
- Sharing of sensitive data with external entities must follow a data sharing agreement that complies with all VCU / VCUHS standards.
- Confidential and protected data must not be stored on non-VCU or non-VCUHS owned devices.
- Sensitive data must be disposed of according to VCU or VCUHS standards.
- If the employee separates from the organization, the data owner must notify the responsible IT system administrator and collect any access tokens, keys or key cards within 24 hours following employee termination.
- Remote access to business IT systems must be encrypted.
- All remote access into the VCU Network must use VCU or VCUHS approved tools (WebVPN, F5, Cisco VPN); exceptions must be approved by the appropriate VCU or VCUHS Information Security Officers.
- The offsite computer used for remote access must meet the Workstation Security Standard.

**Removable Storage Media Security Standard**
- Removable storage media can be moved from workstation to workstation without any physical modification to the computer hardware. Examples of removable storage media include USB drives (thumb drives), CDs / DVDs, Floppy disks, USB or Firewire removable Hard drives, as well as SD, MMC, CF and any other types of storage cards.
- All removable storage media used to store sensitive data must utilize industry approved encryption standard.
- Removable storage media used to store confidential and protected data must be password protected and encrypted to meet the FIPS 140-2 compliant encryption standard.

**Business Continuity Management for IT Systems**
- All critical business functions must have a documented business function owner
- All IT systems supporting critical business functions must have a clearly defined system owner and system administrator.
- All IT systems must be inventoried and documented. The inventory and documentation must be updated annually to reflect changes.
- A business impact analysis and risk assessment must be conducted for each business unit at least once every 3 years.
- A disaster recovery plan must be documented and tested annually.

**Data Breach Notification:**
- Immediately report any unauthorized access, misuse, tampering or deletion of sensitive data to the data owner and / or Information Security Office.
• Immediately report any loss or theft of equipment that contains or has access to sensitive data to the VCU police at 828 – 1196.

<table>
<thead>
<tr>
<th>Contact Information:</th>
<th>Phone</th>
<th>Electronic reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>VCU Police</td>
<td>828 - 1196</td>
<td><a href="http://www.vcu.edu/police/reporter.html">http://www.vcu.edu/police/reporter.html</a></td>
</tr>
<tr>
<td>VCU Helpdesk</td>
<td>828 - 2227</td>
<td><a href="http://supportcenter.vcu.edu">http://supportcenter.vcu.edu</a></td>
</tr>
<tr>
<td>VCUHS Helpdesk*</td>
<td>828 - 6447</td>
<td><a href="http://isservicedesk-test.mcvh-vcu.edu/rapidwebsubmittal/">http://isservicedesk-test.mcvh-vcu.edu/rapidwebsubmittal/</a></td>
</tr>
<tr>
<td>VCU SOM Security</td>
<td>827 - 9907</td>
<td><a href="mailto:somsecurity@vcu.edu">somsecurity@vcu.edu</a></td>
</tr>
</tbody>
</table>

*The VCUHS Helpdesk electronic reporting site is only accessible from VCUHS internal network or VCU SecureNet networks.