Title: Data Classification Guidelines

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>November 18, 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 purpose of this document is to help all VCU School of Medicine personnel to define the sensitivity of the data they access, in accordance with the VCU Information Security Standards and the VCUHS Affiliated Covered Entity Information Security policies.

II. GUIDELINE
The VCU School of Medicine has three data classification categories. Ranging from the most sensitive to the least, these categories include: confidential and protected, sensitive, and non-sensitive. All VCU School of Medicine data must be handled according to the VCU School of Medicine data handling and storage standards. This guideline will provide the qualifications on data of each classification.

III. 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.

IV. QUALIFICATION FOR CONFIDENTIAL AND PROTECTED DATA
Data in this category 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. 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 typically include, but are not limited to personally identifiable information or information that contains identifiers, or a set of identifiers that allows the identification of an individual. Examples of confidential and protected data include:

Social Security Numbers
Account login name and password
Personal identification numbers (PIN)
Personal characteristics (Finger print, Retina, X-ray, other biometric image)
Vehicle registration or identification number
Passport or visa numbers
Research data that can be used to identify human subjects
Research data covered by non-disclosure agreements
Financial Account Numbers, such as Credit Card Numbers / Bank Account Numbers
Privileged attorney client communications
Medical records related to an individual
Psychological Counseling records related to an individual
Trade secrets or intellectual property
any combination of above information that can be linked back, no matter how brief, to an individual

V. QUALIFICATION FOR SENSITIVE DATA
Sensitive data are releasable under the Commonwealth of Virginia Information Act, and / or are regulated by the University or School policies or standards. Such data include salary, contents of specific email or departmental calendars. Further, business data that are proprietary to the institution, including proprietary and properly de-identified research data are also considered sensitive. Loss of these data may result in short-term loss of reputation and research funding. The sensitive data must be properly protected. Examples of sensitive data include:

Proprietary research data
Non-public contracts
Faculty/staff employment applications, personnel files, date of birth, and personal contact information
Employee salary and benefits information
Employee performance evaluation
Employee work profile
Admissions applications
Business project information
Non-public policies and policy manuals
Internal memos and email, and non-public reports, budgets, and plans
Donor contact information and non-public gift amounts
Large number of e-mail addresses
Vulnerability/security information related to the campus or a system
Location of assets such as hazardous materials

VI. QUALIFICATION FOR NON-SENSITIVE DATA
Non-sensitive data are 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. The types of non-sensitive data are listed below:

A. Non-Sensitive Business Data – These data are not protected by trademark or patent or copyright, are available in the public domain and anyone can produce or distribute them. These data have no existing local, national or international legal restrictions on access or usage. Non-Sensitive Business data are available to all members of the University community and to all individuals and entities external to the University community. Examples of such data include publicly available non-proprietary research data, publicly posted press releases, publicly posted schedule of classes, publicly posted newsletters or magazines, directory information (unless suppressed or restricted), research blogs, and data generated by research instruments that can be easily recreated.
B. **Personal data** – These data are not related to any business tasks in the University. These data typically belong to a specific individual, and only relate to that specific individual. Examples of such data include: personal bookmarks of internet sites, personal play list of music, photos, and personal notes.