Title: Business Continuity Management Standard for IT Systems

Scope: This standard is applicable to all VCU School of Medicine departments and divisions.

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>February 25, 2010</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 member feedback</td>
</tr>
</tbody>
</table>
I. **PURPOSE**
The Business Continuity Management Standard establishes the basic framework necessary to ensure VCU School of Medicine’s continuity of business operations during a business interruption event.

II. **POLICY**
Various business functions exist that are critical to the VCU School of Medicine mission. All business functions must be identified and the criticality of these business functions must be properly defined. In order to ensure the minimum impact to the business and the continuity of operations in event of interruption, plans for recovery and continuity of operations must be defined, documented and periodically revised for all essential business functions. This document defines the business continuity management methodologies for IT systems that support the critical business functions.

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.

- **Business Function** – A collection of related structural activities that produce something of value to the organization, its stakeholders or its customers. Examples of business functions include HR, Accounts Receivable, Desktop Support etc.

- **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.

**Essential Business Function** – A business function is essential, or critical if disruption or degradation of the function prevents the agency from performing its mission as described in the agency mission statement.

**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.

**Maximum Tolerable Downtime (MTD)** - the maximum time a business can tolerate the absence or unavailability of a particular business function. Maximum Tolerable Downtime is comprised of Recovery Time Objective and Work Recovery Time.

**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.

**Recovery Time Objective (RTO)** – The period of time in which systems, applications or functions must be recovered after an outage. The RTO is the first part of the Maximum Tolerable Downtime (MTD)

**Recovery Point Objective (RPO)** - The measurement of the point in time to which data must be restored in order to resume processing transactions. Directly related to the amount of data that can be lost between the point of recovery and the time of the last data backup.

**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.

**Structured Walk-Through** – A disaster recovery testing methodology that allows all disaster recovery personnel in functional areas to come together to identify and correct weaknesses in a disaster recovery plan.
System Owner – A VCU or VCUHS employee who is responsible to authorize or deny access to computer workstations to system users. The system owners are directly responsible for the physical and logical security of the computer workstations that are under their control.

System User – A VCU or VCUHS personnel who is authorized by the System Owner to have access to a VCU School of Medicine computer workstation. A system user can consist of faculty members, graduate students, post doctoral associates, staff members, vendors, external organization users, and any other affiliates who have access to a VCU School of Medicine computer workstation.

Threat - Any circumstance or event (human, physical, or environmental) with the potential to cause harm to an IT system in the form of destruction, disclosure, adverse modification of data, and/or denial of service by exploiting vulnerability.

Vulnerability - A condition or weakness in security procedures, technical controls, or operational processes that exposes the system to loss or harm.

Work Recovery Time (WRT) – The amount of time it takes to get critical business functions back up and running once the systems (hardware, software, and configuration) are restored. The WRT is the second half of Maximum Tolerable Downtime (MTD)

IV. RESPONSIBILITIES

All VCU School of Medicine business function owners who support essential business functions are responsible to read and understand the standards set forth in this document. Further, the system users of IT systems that support these essential business functions are responsible to review and understand the continuity of operations and disaster recovery procedures associated with the IT systems that are used.

The data owner of sensitive data is directly responsible for the confidentiality, integrity and security of the data stored, processed, and/or transmitted via any communication medium.

The business function owner in conjunction with system owners and the respective data owners are responsible for defining and documenting the essential VCU School of Medicine business functions under their control, initiating and coordinating the risk management process, and developing a continuity of operations and disaster recovery plan for the identified essential business functions.
The VCU School of Medicine Information Security Manager is responsible for reviewing and auditing this standard annually.

V. BUSINESS IMPACT ANALYSIS

A. A business function owner must be identified and documented for each essential business function in the VCU School of Medicine.

B. Business function owners must identify and document VCU School of Medicine business functions, the respective functional dependencies, and classify each function according to how essential it is based on the potential impact on VCU School of Medicine’s mission if there was disruption or degradation of the function.

C. Business function owners must determine and document the Maximum Tolerable Downtime, Recovery Time Objective, Work Recovery Time, and Recovery Point Objective for each essential business function.

D. Business function owners in conjunction with system owners and data owners must identify and document the appropriate IT resources that support each essential business function.

E. A system owner, data owner, and system administrator must be identified and documented for each IT system that contains or has access to sensitive data.

F. Business Impact Analysis must be conducted once every three years for all essential business functions.

VI. RISK MANAGEMENT

A. All VCU School of Medicine IT systems used to access, process or store sensitive data must be inventoried and documented.

B. At a minimum, IT systems inventory for each business unit must be updated on an annual basis.

C. All IT systems that are deemed to support essential business functions and/or store or process confidential and protected data must undergo a formal risk assessment every three years.

D. All IT systems that are deemed to support essential business functions and/or store or process confidential and protected data must undergo annual self-assessment to determine the continued validity of the formal Risk Assessment.
E. A report of each Risk Assessment must be documented that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, the associated threats, including the likelihood of exploitation, and an executive summary, including major findings and risk mitigation recommendations.

VII. CONTINUITY OF OPERATIONS

A. Based on results from the Business Impact Analysis and Risk Assessment, documented onsite and offsite backup and recovery requirements must be defined and maintained for IT systems that support essential business functions and/or store or process confidential and protected data.

B. A disaster recovery plan must be documented for IT systems that support essential business functions and/or store or process confidential and protected data. At a minimum, the plan must include plan activation requirements, resources and personnel needed for recovery, documented responsibilities and procedures for each resource and personnel, and a clear recovery timeline that is equal to or less than the Recovery Time Objective.

C. Personnel contact information and incident notification procedures must be clearly documented and shared with all disaster recovery personnel, the system owner, system administrator and all data owners of the system.

D. Annual test of the disaster recovery and continuity of operations procedures must be conducted for IT systems that support essential business functions and/or store or process confidential and protected data. The minimum acceptable testing methodology is a structured walk-through.

E. Annual review of the continuity plan and disaster recovery plan must be conducted for IT systems that support essential business functions and/or store or process confidential and protected data.

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 Business Continuity Management standard is the responsibility of all owners of essential VCU School of Medicine business functions. 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.

X. REFERENCES
A. VCU Information Security Standard section 2: Risk Management
B. VCU Information Security Standard section 3: IT Contingency Planning
B. VCU Affiliated Covered Entity ACE-002: Security Management Process
C. VCU Affiliated Covered Entity ACE-009: Contingency Plan
D. NIST Special Publication 800-18 Revision 1: Guide for Developing
   Security Plans for Federal Information Systems
## 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: _______________________________________________________________________

<table>
<thead>
<tr>
<th>SOM Information Security Manager Use Only</th>
</tr>
</thead>
<tbody>
<tr>
<td>Approval:</td>
</tr>
<tr>
<td>_ Approved  _ Denied</td>
</tr>
<tr>
<td>_ VCU/VCUHS Approval Required</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