

**Virginia Commonwealth University
Technology Services**

Electronic Sensitive Information Security Management Standards

Business Associates and Contracted Sites

**Technology Services Policy, Procedures and Standards Manual
Volume V: Facility Security**

Version	Date	Revision Issuance
1.0		Initial draft to the VCU Security Web Page
1.1	January 2006	Approval by CIO

PREFACE

Designation:	Technology Services Standard: SEC500-505.1 Business Associates / Contracted Sites
Effective Date:	March 1, 2006
Compliance Date:	March 1, 2006
Supersedes:	
Authority:	VCU Chief Information Officer and VCU Information Security Officer
In Compliance with:	VCU Academic Policy: Security of Electronic Sensitive Information VCU Academic Policy: Information Security Policy UITAC Goals: <i>Infrastructure Goal 1</i> . COV ITRM Information Technology Security Management Standard SEC501-01- 7.5 COV ITRM Information Technology Security Management Policy SEC500-02 VCU-Affiliated Covered Entity Security Policies (Pending Interim Draft)

General Responsibilities:

VCU Information Security Officer:

The VCU Information Security Officer has the duty and responsibility to develop, issue and maintain policies, procedures and standards for the security of University computing assets, the facilities that house these assets and electronic sensitive information that is created on behalf of the University by business associates or contracted sites.

Scope:

This standard is applicable to all University contracted Business Associates and Contracted Sites that are performing work on behalf of the University or that are used for business support that involves electronic sensitive information with connection to any University network.

Purpose:

To define the performance expectations, or processes that must be in place to provide for the security, safeguarding and protection of any University owned electronic sensitive information that is created, received, used, disclosed, maintained or transmitted by a contracted business associate, or affiliated¹ site and that these business associates provide written assurances that their information systems remain secure.

Regulatory Compliance References:

The standards of this document respond to and address compliance to the following State of Virginia Information Technology Security Management standards and the federal HIPAA Security and Privacy Rule standards.

- COV ITRM SEC501-01, Section 7.5 Mandates that written contractual assurances be in place for the protection of sensitive information and the information hardware it is maintained on as well as networks used for the transmission of sensitive information are secure and protected.
- COV ITRM SEC501-01, Section 10.2.2 Security of Mission Critical Systems Facilities.
- HIPAA Security Rule, §164.308(b)(1) Standard: Business Associate Contracts and Other Arrangements.
- HIPAA Privacy Rule, §164.504(e)(1) Standard: Business Associate Contracts.

Definition: COV ITRM SEC501-01

¹ "Affiliation" with the University implies that the affiliated entity has established a written agreement that has been approved by the VCU Office of the General Counsel and Board of Visitors for the purpose of the establishment of a scholarly affiliation with the University having a mission of providing clinical care; or enhancing scientific knowledge through investigation; and / or providing education and training to students and professionals.

There is no formal State definition of a "Contracted Site". In the absence of a State policy definition this Technology Services standard adopts the HIPAA definition of "Business Associate" to include any contracted site having a written agreement with the University to perform a scope-of-work.

HIPAA Privacy and Security Rules

"Business Associate": A person or entity other than a member of the covered entity's (VCU-ACE) workforce, who performs a function for or assists a covered entity with a function that involves the use or disclosure of individually identifiable health information (sensitive information).

These *Business Associate and Contracted Sites* standards focus on the information security management processes that are identified within contracted service agreements or arranged through other types of written agreements. These written agreements must contain assurances by the business associate that:

1) The business associate plans and designs information technology management processes to meet the security and confidentiality standards of the University, state policy and the federal HIPAA Privacy and Security Rules; 2) Confidentiality, security, and integrity of electronic sensitive information owned by the University is respected and maintained; 3) Transmission of electronic sensitive information is over secure networks; 4) University owned electronic sensitive information is protected against loss, theft, destruction, tampering, and unauthorized use or disclosure.

The **standard** is a statement that *defines the performance expectations or processes that must be in place* in order for the University to maintain a secure and protected environment for sensitive information that is maintained within the care and custody of business associates.

The elements of performance for each standard *are the specific performance expectations or processes* that must be in place in order for the Unit that is contracting with the business associate to meet these standards.

Standard S.1.0 Roles of individuals and the responsibilities of the business associate's workforce for the security of University sensitive information are clearly identified within a written agreement.

1.1 All Business associates that have care, use and custody of University sensitive information provide their workforce with appropriate training and education on their information security responsibilities.

Standard S.2.0 Physical security of University owned sensitive information and mission critical information systems is reasonably and appropriately maintained.

2.1 Electronic sensitive information and mission critical information systems are located within secure facilities in areas that are protected against trespass, unauthorized access and are safeguarded against physical or electronic intrusion.

Standard S.3.0 Business associates provide assurances for maintaining the continuity of information.

3.1 Business associates maintain a business continuity / disaster recovery plan for University owned electronic sensitive information and University owned information technology assets that are in the care and custody of the business associate. These business continuity plans include the identification of the most critical information and the impact on the University if the business associate services were severely interrupted.

Standard S.4.0 The network connectivity between the business associate site and the University is subject to prior review and written approval by the University's Technology Services Department.

Standard S.5.0 The business associate has written assurances contained within the service agreement language that provides for the following performance conditions to be included within the contracted scope-of-work.

- 5.1 All business associates shall have background screening of personnel consistent with the sensitivity of the data to which the business associates have access; and shall provide notarized or certified evidence of such screening upon request by the University.
- 5.2 Business associates shall comply with the information security policies and procedures of the Technology Services Department; and if electronic protected health information is used or disclosed then the information security policies of the VCU-Affiliated Covered Entity are considered for compliance.
- 5.3 Based upon the sensitivity of the information, the Auditor of Public Accounts, the University's Information Security Officer or the VCU-ACE Security Officer shall be allowed to visit the business associate site to conduct assessments, validation reviews and audits of the business associate sites and systems that are used to provide sensitive information technology services to the University.
- 5.4 Non-disclosure agreements shall be used to protect electronic sensitive information in accordance with the information classification requirements as issued by the Department of Technology Services.