

**High Level Crosswalk Mapping
Virginia Information Technology Security
Management Standard (SEC501-01)
And
Current VCU Security
Standards/Policies/Procedures**

Background

The Information Technology Security Management Standard (SEC 501-01/ Revision 3) dated July 1, 2007 is the current document produced by the Virginia Information Technologies Agency (VITA) with an effective date of July 1, 2007. The compliance date is July 1, 2008 for new and substantively revised requirements, and November 1, 2007 for sections 9.5.2 (3 through 6)

In June 2007, VITA granted an extension for compliance until September 28, 2007 except for designation of the Information Security Officer which was due July 1, 2007.

The intent of this standard is to establish a baseline of information technology security control and to validate that security controls are in place that address, without limitation, the requirements of all statues and best practices list on page ii of the standards document. The standard defines the minimum acceptable level of information security and Virginia agencies and institutions must implement a security program that complies with this standard.

Document History:

Initial document – 11/06

Updated – 10/07

Updated – 12/07

Std	SEC 501-01	VCU Security Standards/Policies
1.1	Intent	
1.2	Organization of this Standard	<ul style="list-style-type: none"> ▪ Technology Services Organization Chart
1.3	Roles and Responsibilities	
1.4	IT Security Policy and Program	<ul style="list-style-type: none"> ▪ VCU Information Security Program
1.5	Exceptions to Security Requirements	<ul style="list-style-type: none"> ▪ Security Standard Request for Exception (document on website)
1.6	Exemptions from Applicability	
2	Risk Management	
2.1	Purpose: identify, analyze, prioritize and mitigate risks that could compromise systems. Defines standards in seven areas:	
2.2	<ul style="list-style-type: none"> ▪ IT Security Roles and Responsibilities – steps taken to establish formal roles and assign responsibilities to manage and protect IT systems 	<ul style="list-style-type: none"> ▪ Designation of ISO and backup ISO
2.3	<ul style="list-style-type: none"> ▪ Business Impact Analysis – steps to identify business 	<ul style="list-style-type: none"> ▪ Server Registry

<p>2.4</p> <p>2.5</p> <p>2.6</p> <p>2.7</p>	<p>functions that are essential to mission and identify resources required to support these functions</p> <ul style="list-style-type: none"> ▪ IT System and Data Sensitivity Classification ▪ Sensitive IT System Inventory and Definition ▪ Risk Assessment ▪ IT Security Audits classify data handled to BIA process and/or which handles sensitive data 	<ul style="list-style-type: none"> ▪ VCU Data Classification Guidelines; Security Standard for Electronic Confidential Information and Privacy Standard ▪ Social Security Number Policy; Sensitive Data Registry ▪ Risk Assessments of sensitive areas/systems ▪ Internal audits
<p>3</p> <p>3.1</p> <p>3.2</p> <p>3.3</p> <p>3.4</p>	<p>IT Contingency Planning Purpose: Delineates steps necessary to plan for and execute recover and restoration of IT systems and data if an event occurs that renders IT systems and/or data unavailable. Covers requirements in three areas:</p> <ul style="list-style-type: none"> • Continuity of Operations Planning • IT Disaster Recovery Planning • IT System and Data Backup and 	<ul style="list-style-type: none"> ▪ Emergency Preparedness Plan Incident Handling Procedures • Disaster Recovery Plan ▪ Backup/Restore Procedures; Tape Protection Procedures
<p>4</p> <p>4.1</p> <p>4.2</p>	<p>IT Systems Security Purpose: Delineates steps to protect IT systems in five areas:</p>	

5.3	<ul style="list-style-type: none"> ▪ Password Management 	<ul style="list-style-type: none"> • Administration Procedures • Security Standard for Passwords; Use of Person Database Standard; eID Password Enforcement Policies
5.4	<ul style="list-style-type: none"> ▪ Remote Access 	<ul style="list-style-type: none"> • Security Standard for Remote Access
6	<p>Data Protection Purpose: Delineate steps to protect COV data from improper or unauthorized disclosure. Defines requirements in two areas:</p>	
6.1		
6.2	<ul style="list-style-type: none"> • Data Storage Media Protection 	<ul style="list-style-type: none"> • Secure University Computer Center; Security Standard for Transmission of Confidential Data Through Email; Security Standard for Confidential Information and Privacy
6.3	<ul style="list-style-type: none"> • Encryption 	<ul style="list-style-type: none"> • Security Standard for Encryption, Security Standard for Remote Access and various other standards that require encryption for logons and confidential data
7	<p>Facilities Security Purpose: Identify steps necessary to safeguard the physical facilities that house IT equipment, systems, services and personnel.</p>	
7.1		
7.2	<ul style="list-style-type: none"> ▪ Requirements: <ol style="list-style-type: none"> 1. Safeguard IT systems and data residing in static facilities, mobile facilities and portable facilities. 2. Design safeguards to protect against human, natural and 	<ul style="list-style-type: none"> • Physical Access Controls: Access Cards/ID Verification

	<p>environmental risks</p> <ol style="list-style-type: none"> 3. Require appropriate environmental controls 4. Protect against physical access by unauthorized personnel 5. Control physical access to essential computer hardware, wiring, displays and networks by principle of least privilege 6. Provide a system of monitoring and auditing physical access to sensitive IT systems 7. Require that ISO periodically review the list of persons allowed physical access to sensitive IT systems 	<ul style="list-style-type: none"> • Security Standard for the Wireless Network
<p>8 8.1</p>	<p>Personnel Security Purpose: Delinates steps necessary to restrict access to IT systems and data to those individual who require such access as part of their job duties. Defines requirements in three areas:</p>	
<p>8.2</p>	<ul style="list-style-type: none"> ▪ Assess determination and control – 	<ul style="list-style-type: none"> • Access Cards/ID Verification
<p>8.3</p>	<ul style="list-style-type: none"> ▪ IT Security Aawareness and Training – 	<ul style="list-style-type: none"> • Role-based Security Awareness Modules (pilot)
<p>8.4</p>	<ul style="list-style-type: none"> ▪ Acceptable use 	<ul style="list-style-type: none"> • Computer and Network Resources Use Policy
<p>9 9.1</p>	<p>Threat Management Purpose: Delineates steps necessary to protect IT systems and data by preparing for and responding to IT security incidents. Defines requirements in four areas:</p>	
<p>9.2</p>	<ul style="list-style-type: none"> ▪ Threat detection – prevention 	<ul style="list-style-type: none"> ▪ Security Appliances – IDS/IPS, NetFlow Analyzer; Cisco Security Monitoring, Analysis and Response System (MARS); Security

<p>9.3</p> <p>9.4</p> <p>9.5</p>	<ul style="list-style-type: none"> ▪ IT Security Monitoring and Logging ▪ IT Security Incident Handling ▪ Data Breach Notification 	<p>Standard for Web Servers and Applications</p> <ul style="list-style-type: none"> ▪ Cisco MARS; NetFlow Analyzer, IDSs, vulnerability scanning; Incident Database • Incident Handling Procedures • Data Breach Procedures
<p>10</p> <p>10.1</p> <p>10.2</p> <p>10.3</p> <p>10.4</p>	<p>Asset Management</p> <p>Purpose: Delineates steps necessary to protect IT systems and data by managing the IT assets themselves in a planned, organized and secure fashion. Defines requirements in three areas:</p> <ul style="list-style-type: none"> ▪ IT Asset Control ▪ Software license management ▪ Configuration management and change control – 	<ul style="list-style-type: none"> • Asset Tagging; Procedures for Surplus Equipment Disposal ▪ Software Site License Agreements; DMCA Procedures ▪ Change Management