Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
1.3	**Roles and Responsibilities** Descriptions of key IT security roles and responsibilities are included in the current version of the *Information Technology Security Policy* (COV ITRM Policy SEC500). Each agency must maintain an organization chart that depicts the reporting structure of employees with specific responsibilities for the security of IT systems and data and their specific IT security roles and responsibilities.	Agency	
1.4	**IT Security Program** Each Agency shall establish, document, implement, and maintain its IT security program appropriate to its business and technology environment in compliance with this *Standard* . In addition, because resources that can reasonably be committed to protecting IT systems are limited, each Agency must implement its IT security program in a manner commensurate with sensitivity and risk.	Agency	
1.5	**Exceptions to Security Requirements** The Chief Information Security Officer of the Commonwealth (CISO) must approve exceptions to this Standard. For each exception, the requesting Agency shall document: □ The business need, □ The scope and extent, □ Mitigating safeguards, □ The specific duration, and □ Agency Head approval. If the CISO denies a request for an exception to this Standard, the Agency requesting the exception may appeal the denial to the Chief Information Officer of the Commonwealth (CIO) through the CISO. The form that Agencies must use to document such exception requests is included as the Appendix to this document.	Agency	
1.6	**Exemptions from Applicability** The following are explicitly exempt from complying with the requirements defined in this document: a. Systems under development and/or experimental systems that do not create additional risk to production systems b. Surplus and retired systems	Agency	
2.2.2 Requirements	Each Agency Head shall:		
1	1. Designate an Information Security Officer (ISO) for the agency, and provide the person's name, title, and contact information to the CISO via email to VITASecurityServices@vita.virginia.gov no less than biennially. The Agency Head is strongly encouraged to designate at least one backup for the ISO. Agencies with multi-geographic locations or specialized business units should also consider designating deputy ISOs as needed.	Agency	
	Each Agency Head or designated ISO Shall:		
1	Assign individuals to the roles described in the current version of the *Information Technology Security Policy* (COV ITRM Policy SEC500).	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
2	Document the responsibilities of the designee for each role identified.	Agency	
3	Review System Security Plans (Section 4.2) for all sensitive agency IT systems (Section 2.4) and: a. Approve those System Security Plans that provide adequate protections against IT security risks; or b. Disapprove System Security Plans that do not provide adequate protections against IT security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against IT security risks	Agency	
4	Prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that: a. The ISO is not a System Owner or a Data Owner except in the case of compliance systems for IT Security; b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and c. The ISO, System Owners, and Data Owners are COV employees.	Agency	
5	Review the position descriptions of all employees assigned to IT security roles annually, or more often as necessary, and verify that the position descriptions accurately reflect assigned IT security duties and responsibilities.	Agency	
2.3.2 Requirements	Each Agency shall:		
1	Require the participation of System Owners and Data Owners in the development of the agency's BIA.	Agency	
2	Identify Agency business functions.	Agency	
3	Identify essential business functions.	Agency	
4	Identify dependent functions. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.	Agency	
5	For each essential business function: • Determine and document the required Recovery Time Objectives (RTO) for each ~~essential business~~ function, based on agency and COV goals and objectives. • Determine and document the Recovery Point Objectives (RPO) for each essential business function. • Identify the IT resources that support each essential business function.	Agency	
6	Use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification (Section 2.4), Risk Assessment (Section 2.6), and IT Contingency Planning (Section 3).	Agency	
7	Conduct periodic review and revision of the Agency BIA, as needed, but at least once every three years.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
2.4.2 Requirements	Each Agency ISO shall:		
1	Identify or require that the Data Owner Identify the type(s) of data handled by each agency IT system.	Agency	
2	Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements.	Agency	
3	Determine or require that the Data Owner determine the potential damages to the Agency of a compromise of confidentiality, integrity or availability of each type of data handled by the IT system, and classify the sensitivity of the data accordingly.	Agency	
4	Classify the IT system as sensitive if any type of the data handled by the IT system has a sensitivity of high on any of the criteria of confidentiality, integrity, or availability.	Agency	
5	Review IT system and data classifications with the Agency Head or designee and obtain Agency Head or designee approval of these classifications.	Agency	
6	Verify and validate that all agency IT systems and data have been classified for sensitivity.	Agency	
7	Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users.	Agency	
8	Require that the agency prohibit posting any data classified as sensitive with respect to confidentiality on a public web site, ftp server, drive share, bulletin board or any other publicly accessible medium unless a written exception is approved by the Agency Head identifying the business case, risks, mitigating logical and physical controls, and any residual risk.	Agency	
9	Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process (Section 2.6).	Agency	
2.5.2 Requirements	Each Agency ISO shall:		
1	Document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.	Agency	
2	Assign a System Owner, Data Owner(s), and System Administrator(s) for each Agency-owned sensitive IT system.	Agency	
3	Maintain or require that its service provider maintain updated network diagrams.	Agency with ISP	ISP provide technical advice and assistance to help define boundaries
2.6.2 Requirements	For each IT system classified as sensitive, the data owning agency shall:		
1	Conduct a formal RA of the IT system, as needed, but not less than once every three years.	Agency with ISP	ISP provide technical advice

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
2	Conduct an annual self-assessment to determine the continued validity of the formal RA.	Agency with ISP	ISP provide technical advice and provide information on threats to IT Systems
3	Prepare a report of each RA that includes, at a minimum, identification of all vulnerabilities discovered during the assessment, and an executive summary, including major findings and risk mitigation recommendations.	Agency	
2.7.2 Requirements	For each IT system classified as sensitive, the data owning agency shall:		
1	1. Require that the IT systems undergo an IT Security Audit as required by and in accordance with the current version of the *IT Security Audit Standard* (COV ITRM Standard SEC502).	Agency	
2	Assign an individual to be responsible for managing IT Security Audits.	Agency	
3.2.2 Requirements	Each Agency shall:		
1	Designate an employee to collaborate with the Agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery planning activities.	Agency	
2a.	Based on BIA and RA results, develop Agency COOP IT-related documentation which identifies: a. Essential business functions that require restoration and the Recovery Time Objective (RTO) for each;	Agency	
2b.	b. Recovery requirements for IT systems and data needed to support the essential business functions; and	Agency with ISP	ISP provide technical advice and provide IT Systems Technical specifications
2c.	c. Personnel contact information and incident notification procedures.	Agency with ISP	ISP's VCCC
3	Require an annual exercise (or more often as necessary) of IT COOP components to assess their adequacy and effectiveness.	Agency with ISP	Only where IT technical is involved
4	Require review and revision of IT COOP components following the exercise (and at other times as necessary).	Agency with ISP	Provide technical assistance
3.3.2 Requirements	Each Agency shall:		
1	Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions.	Agency with ISP	ISP advise for providing input to technical specifications Combine with 2b above under 3.2.2
2	Require approval of the IT DRP by the Agency Head.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
3	Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.	Agency with ISP	ISP assist with technical IT revisions
4	Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.	Agency with ISP	ISP advise for Technical communication methods
3.4.2 Requirements	For every IT system identified as sensitive, each Agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems and data in accordance with Agency requirements. At a minimum, these plans shall address the following:		
1	Secure off-site storage for backup media.	ISP	
2	Store off-site backup media in an off-site location that is geographically, separate and distinct from the primary location.	ISP	
3	Performance of backups only by authorized personnel.	ISP	
4	Review of backup logs after the completion of each backup job to verify successful completion.	ISP	
5	Approval of backup schedules of a system by the System Owner.	Agency	
6	Approval of emergency backup and operations restoration plans by the System Owner.	Agency with ISP	Agency approves with ISP advising ISP will provide technical alternatives to backup schedules
7	Protection of any backup media that is sent off site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with Agency requirements.	ISP	Agency must provide requirements
8	Authorization and logging of deposits and withdrawals of all media that is stored off-site.	ISP	
9	Retention of the data handled by an IT system in accordance with the agency's records retention policy.	Agency with ISP	Agency must provide retention schedule
10	Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.	Agency with ISP	ISP provide IT technical advice
4.2.2 Requirements	Each System Owner of a sensitive IT system shall:		
1	Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of: a. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls; b. How these controls provide adequate mitigation of risks to which the IT system is subject.	Agency with ISP	ISP provide technical assistance relative to controls
2	Submit the IT System Security Plan to the Agency Head or designated ISO for approval.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
3	Plan and document additional IT security controls for the IT system if the Agency Head or designated ISO disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.	Agency with ISP	ISP provide technical assistance relative to controls
4	Update the IT System Security Plan every three years, or more often if necessary, and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.	Agency with ISP	ISP provide technical assistance relative to controls
4.3.2 Requirements	Each Agency shall or shall require that its service provider:		
1	Identify, document, and apply appropriate baseline security configurations to Agency IT systems, regardless of their sensitivity.	Agency with ISP	Application: Agency Infrastructure: ISP
2	Identify, document, and apply more restrictive security configurations for sensitive Agency IT systems, as necessary.	Agency with ISP	Agency to identify the more restrictive controls
3	Maintain records that document the application of baseline security configurations.	ISP	
4	Review and revise all security configuration standards annually, or more frequently, as needed.	ISP	
5	Reapply all security configurations to Agency-owned IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.	Agency with ISP	Agency must coordinate with applications
6	Require periodic vulnerability scanning of IT systems in a manner commensurate with sensitivity and risk, to verify whether security configurations are in place and if they are functioning effectively.	Agency with ISP	Agency responsible for application scanning
7	Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.	Agency with ISP	
4.4.2 Requirements	For every sensitive Agency-owned IT system, the Agency ~~shall or~~ shall require or shall specify that its service provider require:		
1	The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:	Agency	
1a.	a. The types of shared data;	Agency	
1b.	b. The direction(s) of data flow; and	Agency	
1c.	c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.	Agency	
2	The System Owners of the IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
3	The System Owners of the IT systems that share data inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.	Agency	
4	The written agreement specify if and how the shared data will be stored on each IT system.	Agency	
5	The written agreement specify that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data.	Agency	
6	The written agreement maintains each Data Owner's authority to approve access to the shared data.	Agency	
7	The System Owners approve and enforce the agreement.	Agency	
4.5.2 Requirements	Each Agency shall, or shall require that its service provider:		
1	Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spyware, keystroke loggers, phishing software, Trojan horses, etc.).	Agency and ISP	Agency for agency users ISP for technical staff
2	Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.	Agency and ISP	Agency for agency users ISP for technical staff
3	Provide malicious program detection, protection, eradication, logging, and reporting capabilities.	ISP	
4	Provide malicious code protection mechanisms on multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.	ISP	
5	Require malicious program protection that: a. Eliminates or quarantines malicious programs that it detects; b. Provides an alert notification; c. Automatically and periodically runs scans on memory and storage devices; d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device; e. Allows only authorized personnel to modify program settings; and f. Maintains a log of protection activities.	ISP	
6	Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the agency's email system.	ISP	
7	Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.	ISP	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
8	Require all forms of malicious code protection to start automatically upon system boot.	ISP	
9	Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.	ISP	
10	Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shut-down, restoration, notification, and reporting requirements.	Agency and ISP	Agency for agency users ISP for technical staff
11	Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.	Agency and ISP	Agency for agency users ISP for technical staff
12	Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.	Agency and ISP	Agency for agency users ISP for technical staff
13	By written policy, prohibit the installation of software on Agency IT systems until the software is approved by the Information Security Officer (ISO) or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.	Agency and ISP	Agency for agency users ISP for technical staff
14	Establish Operating System (OS) update schedules commensurate with sensitivity and risk.	Agency and ISP	Agency for agency users ISP for technical staff
4.6.2 Requirements	Each Agency shall:		
1	Incorporate IT security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.	Agency	
	Project Initiation		
2	Perform an initial risk analysis based on initial requirements and the business objectives to provide high-level security guidelines for the system developers.	Agency with ISP	ISP technical assistance on proposed infrastructure.
3	Classify the types of data (see Section 2.4) that the IT system will process and the sensitivity of proposed IT system.	Agency	
4	Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.	Agency	
5	Develop an initial IT System Security Plan (see Section 4.2) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.	Agency with ISP	ISP technical assistance on proposed infrastructure.
	Project Definition		
6	Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.	Agency	
7	Incorporate IT security requirements in IT system design specifications.	Agency	
8	Verify that the IT system development process designs, develops, and implements IT security controls that meet the IT security requirements in the design specifications.	Agency with ISP	ISP technical assistance on proposed infrastructure.

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
9	Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.	Agency	
10	Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.	Agency	
	Implementation		
11	Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.	Agency	
12	Conduct a RA (see Section 2.6) to assess the risk level of the IT application system.	Agency with ISP	Provide information on threats to IT Systems
13	Require that the system comply with all relevant Risk Management requirements in Section 2 of this document.	Agency	
14	Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against IT security risks, and comply with the other requirements of Section 4.2 of this document.	Agency with ISP	ISP technical assistance on proposed infrastructure.
	Disposition		
15	Require retention of the data handled by an IT system in accordance with the agency's records retention policy prior to disposing of the IT system.	Agency	
16	Require that electronic media is sanitized prior to disposal, as documented in Section 6.2, so that all data is removed from the IT system.	Agency and ISP	Agency for agency controlled devices ISP for ISP controlled devices
17	Verify the disposal of hardware and software in accordance with the ~~COV~~ *current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).	Agency and ISP	Agency for agency controlled devices ISP for ISP controlled devices
4.7.2 Requirements	Each agency ISO is accountable for ensuring the following steps are followed and documented:		
	Application Planning		
	• Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data. (Section 2.4)	Agency	
	• Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be conducted before development begins and after planning is complete. (Section 2.6.2)	Agency	
	• Security Requirements – Identify and document the security requirements of the application early in the development life cycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
	• Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication and access control, and logging requirements.	Agency	
	• Security shall be addressed at all life cycle stages of the system development life cycle (SDLC).	Agency	
	Application Development - The following requirements represent a minimal set of coding practices, which shall be applied to all applications that utilize un-trusted data.		
	• Input Validation – Validate input from all sources. Input validation to be tested should always consider expected and unexpected input, and not block input based on arbitrary criteria.	Agency	
	• Default deny – Access control should be based on specific permission rather than exclusion. By default all access should be denied.	Agency	
	• Principle of Least Privilege – All processes should be performed with the least set of privileges required to complete the process.	Agency	
	• Quality Assurance – Quality assurance is one of the single most effective means of identifying and eliminating software vulnerabilities. Internal testing shall include at least one of the following: penetration testing, fuzz testing, or source code auditing. External source code auditing and/or penetration testing shall be conducted commensurate with sensitivity and risk.	Agency	
	Production and Maintenance		
	• Applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening (Section 4.3.2).	Agency and ISP	Application: Agency Infrastructure: ISP
	Applications classified as sensitive shall at a minimum have annual vulnerability scans run against the applications and supporting server infrastructure and when any significant change to the environment or application has been made.	Agency and ISP	Application: Agency Infrastructure: ISP
5.2.2 Requirements	Each Agency shall or shall require that its service provider document formal account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:		
	For all internal and customer-facing IT systems:		
1	Grant IT system users' access to IT systems and data based on the principle of least privilege.	Agency and ISP	Application: Agency Infrastructure: ISP
2	Define authentication and authorization requirements, based on sensitivity and risk.	Agency and ISP	Application: Agency Infrastructure: ISP
3	Establish policies and procedures for approving and terminating authorization to IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
4	Require requests for and approvals of emergency or temporary access to all sensitive IT systems that: a. Are documented according to standard practice and maintained on file; b. Include access attributes for the account. c. Are approved by the System Owner and communicated to the ISO; and d. Expire after a predetermined period, based on sensitivity and risk.	Agency and ISP	Application: Agency Infrastructure: ISP
5	Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.	Agency with ISP	ISP provide IT technical advice
6	Provide for, review at a consistent frequency, relative to sensitivity and risk, of all user accounts for all IT systems to assess the continued need for the accounts.	Agency and ISP	Agency for agency users ISP for technical staff
7	Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.	Agency and ISP	Agency for agency users ISP for technical staff
8	Prohibit the use of guest and shared accounts on sensitive IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
9	Prohibit the displaying of user's last login name in the logon screen.		
10	Lock an account automatically if it is not used for a predefined period.	Agency and ISP	Application: Agency Infrastructure: ISP
11	Disable unneeded accounts.	Agency and ISP	Application: Agency Infrastructure: ISP
12	Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.	Agency and ISP	Application: Agency Infrastructure: ISP
13	Configure applications to clear cached data and temporary files upon exit of the application or logoff of the system.	Agency and ISP	Application: Agency Infrastructure: ISP
14	Associate access levels with group membership, where practicable, and require that every IT system user account be a member of at least one user group.	Agency and ISP	Application: Agency Infrastructure: ISP
15	Require that the System Owner and the System Administrator investigate any unusual IT system access activities and approve changes to access level authorizations.	Agency and ISP	Application: Agency Infrastructure: ISP
16	Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.	Agency and ISP	Agency for agency system administrators ISP for infrastructure system administrators
17	Require that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.	Agency and ISP	Agency for agency system administrators ISP for infrastructure system administrators
18	Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.	Agency and ISP	Application: Agency Infrastructure: ISP
	For internal IT systems:		

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
19	Require a documented request from the user to establish an account on any internal IT system.	Agency and ISP	Application: Agency Infrastructure: ISP
20	Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.	Agency and ISP	Agency for agency users ISP for technical staff
21	Require employee job descriptions that accurately reflect assigned duties and responsibilities in order to define required IT system access.	Agency and ISP	Agency for agency users ISP for technical staff
22	Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner to establish accounts for sensitive IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
23	Require delivery of access credentials to the user based on information already on file.	Agency and ISP	Application: Agency Infrastructure: ISP
24	Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.	Agency and ISP	Application: Agency Infrastructure: ISP
	For customer-facing IT systems:		
25	Require secure delivery of access credentials to users of all customer-facing IT systems.	Agency	
26	Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of sensitive, customer-facing IT systems.	Agency	
27	Require delivery of access credentials to users of customer-facing sensitive IT systems by means of an alternate channel (i.e., U.S. Mail).	Agency	
5.3.2 Requirements	Password Management Each Agency shall or shall require that its service provider document formal password management practices. At a minimum, these practices shall include the following components:		
1	Require the use of a non-shared and a unique password on each account on IT systems classified as sensitive, including local, remote access and temporary accounts.	Agency and ISP	Agency for agency systems ISP for ISP systems
2	Require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a 4 to 5 digit pin number.	Agency and ISP	Application: Agency Infrastructure: ISP

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
3	Require password complexity • at least eight characters in length, • not be based on a single dictionary word (ex. Bad Password: P4$sw0rD vs. Good Password: t0YtR4p!), and utilize at least three of the following four: • special characters, • alphabetical characters, • numerical characters, • combination of upper case and lower case letters.	Agency and ISP	Application: Agency Infrastructure: ISP
4	Require that default passwords be changed immediately after installation.	Agency and ISP	Application: Agency Infrastructure: ISP
5	Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards (see Section 6.3 – Encryption).	Agency and ISP	Application: Agency Infrastructure: ISP
6	Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.	Agency and ISP	Agency for agency users ISP for technical staff
7	Configure sensitive IT systems to allow users to change their password at will.	Agency and ISP	Application: Agency Infrastructure: ISP
8	Require users of sensitive IT systems to include network systems to change their passwords after a period of 42 days.	Agency and ISP	Application: Agency Infrastructure: ISP
9	Require that IT system users immediately change their passwords and notify the ISO if they suspect their passwords have been compromised.	Agency and ISP	Application: Agency Infrastructure: ISP
10	Maintain the last 24 passwords used in the password history files to prevent the reuse of the same or similar passwords, commensurate with sensitivity and risk.	Agency and ISP	Application: Agency Infrastructure: ISP
11	Provide a unique initial password for each new user of sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner, and require that the IT system user change the initial password upon the first login attempt.	Agency and ISP	Agency for agency users ISP for technical staff
12	Require that forgotten initial passwords be replaced rather than reissued.	Agency and ISP	Agency for agency users ISP for technical staff
13	Prohibit group account IDs and shared passwords on sensitive IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
14	Prohibit the storage of passwords in clear text.	Agency and ISP	Application: Agency Infrastructure: ISP
15	Limit access to files containing passwords to the IT system and its administrators.	Agency and ISP	Application: Agency Infrastructure: ISP

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
16	Suppress the display of passwords on the screen as they are entered.	Agency and ISP	Application: Agency Infrastructure: ISP
17	Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices. COV devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced.	Agency and ISP	Application: Agency Infrastructure: ISP
18	Determine requirements for hardware passwords based on sensitivity and risk.	Agency with ISP	Agency for agency application with ISP advice ISP for firewalls, routers etc.
19	Document and store hardware passwords securely.	Agency and ISP	Application: Agency Infrastructure: ISP
20	Implement procedures to handle lost or compromised passwords and/or tokens.	Agency and ISP	Application: Agency Infrastructure: ISP
5.4.2 Requirements	Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider:		
1	Protect the security of all remote access to the Agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 6.3.	Agency and ISP	Agency Policy ISP Technical solution
2	Protect the security of remote file transfer of sensitive data to and from COV IT systems by means of encryption, in a manner consistent with Section 6.3.	Agency and ISP	Agency Policy ISP Technical solution
3	Document requirements for use of remote access and for remote access to sensitive data, based on agency and COV policies, standards, guidelines, and procedures.	Agency and ISP	Agency Policy ISP Technical solution
4	Require that IT system users obtain formal authorization and a unique user ID and password prior to using the Agency's remote access capabilities.	Agency and ISP	Agency Policy ISP Technical solution
5	Document requirements for the physical and logical hardening of remote access devices.	ISP	
6	Require maintenance of auditable records of all remote access.	Agency with ISP	Agency Policy ISP Technical solution
6.2.2 Requirements	Each Agency shall or shall require that its service provider document Data Storage Media protection practices. At a minimum, these practices must include the following components:		
1	Define protection of stored sensitive data as the responsibility of Data Owner.	Agency with ISP	ISP provide technical assistance

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
2	Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Agency Head that includes the following elements: a. The business or technical justification; b. The scope, including quantification and duration (not to exceed one year) ; c. A description of all associated risks; d. Identification of controls to mitigate the risks, one of which must be encryption; and e. Identification of any unmitigated risks.	Agency and ISP	
3	Require logical and physical protection for all data storage media containing sensitive data, commensurate with sensitivity and risk.	Agency with ISP	ISP provide technical assistance
4	Prohibit the connection of any non-COV owned data storage media or device to a COV-owned network, unless the connection is to a segmented guest network. This prohibition, at the agency's discretion, need not apply to an approved vendor providing operational IT support services under contract.	Agency and ISP	
5	Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing unmitigated risk approved in writing by the Agency Head.	Agency and ISP	
6	Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.	Agency and ISP	Agency controlled data ISP controlled data
7	Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is Personal Health Information (PHI), Personally Identifiable Information (PII), or Critical Infrastructure Information/Sensitive Security Information (CII/SSI). Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.	Agency and ISP	Agency controlled data ISP controlled data
8	Implement processes to sanitize data storage media prior to disposal or reuse.	Agency and ISP	Agency controlled devices ISP controlled devices
	6.3.2 If encryption is in use for the Agency		
6.3.2 Requirements	Commensurate with sensitivity and risk, each Agency shall:		
1	Define and document Agency practices for selecting and deploying encryption technologies and for the encryption of data.	Agency and ISP	ISP provide technical assistance

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
2	Document appropriate processes before implementing encryption. These processes must include the following components: a. Instructions in the IT Security Agency's Incident Response Plan on how to respond when keys are compromised; b. A secure key management system for the administration and distribution of encryption keys; and c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.	Agency and ISP	Agency Policy ISP Technical solution
3	Require encryption during transmission of data that is sensitive relative to confidentiality or ~~and~~ integrity.	Agency and ISP	Agency Policy ISP Technical solution
7.2 Requirements	Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider document facilities security practices. These practices must include the following components, at a minimum:		
1	Safeguard IT systems and data residing in static facilities (such as buildings), mobile facilities (such as computers mounted in vehicles), and portable facilities (such as mobile command centers).	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
2	Design safeguards to protect against human, natural, and environmental risks.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
3	Require appropriate environmental controls such as electric power, heating, fire suppression, ventilation, air-conditioning and air purification, as required by the IT systems and data.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
4	Protect against physical access by unauthorized personnel.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
5	Control physical access to essential computer hardware, wiring, displays, and networks by the principle of least privilege.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
6	Provide a system of monitoring and auditing physical access to sensitive IT systems.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
7	Require that the ISO periodically review the list of persons allowed physical access to sensitive IT systems.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
8.2.2 Requirements	Each Agency shall or shall require that its service provider document access determination and control practices for all sensitive Agency IT systems and all third-party systems with which sensitive Agency IT systems interconnect. At a minimum, these practices shall include the following components:		
1	Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.	Agency	
2	Restrict visitor access to facilities that house sensitive IT systems or data.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
3	Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.	Agency and ISP	Agency for agency users ISP for technical staff
4	Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist, as required in Section 5.2 and Section 7.2.	Agency and ISP	Agency for agency users ISP for technical staff
5	Establish termination and transfer practices that require return of Agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.	Agency and ISP	Agency for agency users ISP for technical staff
6	Temporarily disable physical and logical access rights when personnel are not working for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose.	Agency and ISP	Agency for agency users ISP for technical staff
7	Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.	Agency and ISP	Agency for agency users ISP for technical staff
8	Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of the Agency prohibit a complete separation of duties.	Agency and ISP	Agency for agency users ISP for technical staff
9	Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.	Agency and ISP	Agency for agency users ISP for technical staff
8.3.2 Requirements	Each Agency shall:		
1	Designate an individual who is responsible for all aspects of an Agency's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.	Agency	
2	Include any Agency-specific IT security training requirements in the Agency IT security awareness and training program.	Agency	
3	Require that all IT system users, including employees and contractors, receive IT security awareness training annually, or more often as necessary.	Agency and ISP	Agency for agency users ISP for technical staff
4	Provide additional role-based IT security training commensurate with the level of expertise required for those employees and contractors who manage, administer, operate, and design IT systems, as practicable and necessary.	Agency and ISP	Agency for agency users ISP for technical staff
5	Implement processes to monitor and track completion of IT security training.	Agency and ISP	Agency for agency users ISP for technical staff
6	Require IT security training before (or as soon as practicable after) IT system users receive access rights to the Agency's IT systems, and in order to maintain these access rights.	Agency and ISP	Agency for agency users ISP for technical staff

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
7	Develop an IT security training program so that each IT system user is aware of and understands the following concepts: a. The Agency's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data; b. The concept of separation of duties; c. Prevention and detection of IT security incidents, including those caused by malicious code; d. Proper disposal of data storage media; e. Access controls, including creating and changing passwords and the need to keep them confidential; f. Agency acceptable use policies; g. Agency Remote Access policies; and h. Intellectual property rights, including software licensing and copyright issues.	Agency	
8	Require documentation of IT system users' acceptance of the agency's security policies after receiving IT security training.	Agency	
9	Require specialized IT security training for agency employees, contractors, vendors, business partners, and third parties with specific IT security duties beyond those of all IT systems users as practicable and necessary, including: a. System Owners, Data Owners, and System Administrators; b. IT Disaster Recovery team members; and c. IT Security Incident Response Team members.	Agency and ISP	Agency for agency users ISP for technical staff
8.4.2 Requirements	Each Agency shall:		
1	Document an agency acceptable use policy. Executive branch agencies must adhere to Virginia Department of Human Resource Management Policy 1.75 – Use of Internet and Electronic Communication Systems. Each Executive branch agency shall supplement the policy as necessary to address specific agency needs.	Agency and ISP	Agency for agency users ISP for technical staff
2	Inform IT system users that the COV reserves the right (with or without cause) to monitor, access, and disclose all data created, sent, received, processed, or stored on COV systems.	Agency and ISP	Agency for agency users ISP for technical staff

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
3	3. Limit Local Administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, to only authorized IT staff, as stated in 5.2.2, #~~18,~~ #17, so as to prevent users from: a. Installing or using proprietary encryption hardware/software on COV owned systems; b. Tampering with security controls configured on their workstations; c. Installing personal software on a COV owned system; d. Adding hardware to, removing hardware from, or modifying hardware on a COV system; and e. Connecting non-COV-owned devices to a COV IT system or network, such as personal computers, laptops, or hand held devices, except in accordance with the current version of the Use of non-Commonwealth Computing Devices to Telework Standard (COV ITRM Standard SEC511).	Agency and ISP	Agency for agency users ISP for technical staff and provide technical advice
4	Prohibit the use of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with intellectual property laws governing the materials.	Agency and ISP	
5	Prohibit the transmission of unencrypted sensitive data over the Internet.	Agency and ISP	Agency for agency users ISP for technical staff
6	Require documentation of IT system users' acceptance of the Agency's Acceptable Use Policy before, or as soon as practicable after, gaining access to Agency IT systems.	Agency and ISP	Agency for agency users ISP for technical staff
8.5.3 Requirement	***Email Disclosure Requirements -*** The ISO must consult with the agency's legal counsel before adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such. Following is an example of an email disclaimer for consideration when meeting with your agency's legal counsel. *The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from your computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).* *No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient .*	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
9.2.2 Requirement	Each Agency shall or shall require that its service provider document threat detection practices that include the following components, at a minimum:		
1	Designate an individual responsible for the Agency's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.	Agency with ISP	
2	Conduct Intrusion Detection Systems (IDS) and Intrusion Prevention System (IPS) log reviews to detect new attack patterns as quickly as practicable.	ISP	Infrastructure
3	Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.	Agency with ISP	Infrastructure
4	Maintain regular communication with security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.	Agency and ISP	Application: Agency Infrastructure: ISP
9.3.2 Requirements	Commensurate with sensitivity and risk, each Agency shall, or shall require that its service provider, document IT security monitoring and logging practices that include the following components, at a minimum:		
1	Designate individuals responsible for the development and implementation of IT security logging capabilities, as well as detailed procedures for reviewing and administering the logs.	Agency and ISP	Application: Agency Infrastructure: ISP
2	Enable logging on all IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
3	Monitor IT system event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.	Agency and ISP	Application: Agency Infrastructure: ISP
4	Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.	Agency and ISP	Application: Agency Infrastructure: ISP
5	Prohibit the use of keystroke logging, except when required for security investigations and approved in writing by the Agency Head.	Agency and ISP	Agency for agency users ISP for technical staff
9.4.2 Requirements	Each agency shall document IT security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling practices that include the following components, at a minimum:		
1	Designate an IT Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.	Agency and ISP	
2	Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.	Agency and ISP	
3	Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks.	Agency and ISP	
4	Establish IT security incident categorization and prioritization based on the immediate and potential adverse effect of the IT security incident and the sensitivity of affected IT systems and data.	Agency and ISP	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
5	Identify immediate mitigation procedures, including specific instructions, based on IT security incident categorization level, on whether or not to shut down or disconnect affected IT systems.	Agency and ISP	
6	Establish a process for reporting IT security incidents to the CISO. Executive branch agencies must establish a reporting process for IT security incidents in accordance with §2.2-603(F) of the Code of Virginia so as to report "*to the Chief Information Officer within 24 hours from when the department discovered or should have discovered their occurrence,*" "*all known incidents that threaten the security of the Commonwealth's databases and data communications resulting in exposure of data protected by federal or state laws, or other incidents compromising the security of the Commonwealth's information technology systems with the potential to cause major disruption to normal agency activities.*"	Agency and ISP	
7	Establish requirements for internal Agency IT security incident recording and reporting requirements, including a template for the incident report.	Agency	
8	Establish procedures for incident investigation, preservation of evidence, and forensic analysis.	Agency and ISP	ISP Technical assistance
9	Report IT security incidents only through channels that have not been compromised.	Agency	
9.5.2 Requirements	Each agency shall:		
1	Identify all agency systems, processes, and logical and physical data storage locations (whether held by the agency or a third party) that contain Personal Information which means the first name or first initial and last name in combination with and linked to any one or more of the following data elements, when the data elements are neither encrypted nor redacted. a. Social security number b. Drivers license number or state identification card number issued in lieu of a driver's license number. c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts. d. Other personal identifying information, such as insurance data or date of birth. "Redact" means alteration or truncation of data such that no more than the following are accessible as part of the information: a. Five digits of a social security number; or b. The last four digits of a driver's license number, state identification card number, or account number.	Agency with ISP	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	Responsibility	Comment
2	Include provisions in any third party contracts requiring that the third party and third party subcontractors: a. Provide immediate notification to the agency of suspected breaches; and b. Allow the agency both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.	Agency	
3	Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted Personal Information by any mechanism, including, but not limited to: a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc. b. Theft or loss of physical hardcopy c. Security compromise of any system. An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key. If a data custodian is the entity involved in the data breach they must alert the data owner so that the data owner can notify the affected individuals. The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #8, below.	Agency	
4	In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of that computer must be alerted in accordance with data breach rules.	Agency	
5	Provide notification that consists of: a. A general description of what occurred and when; b. The type of personal information that was involved; c. What actions have been taken to protect the individual's personal information from further unauthorized access; d. A telephone number that the person may call for further information and assistance, if one exists; and e. What actions the agency recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
6	Provide this notification by one or more of the following methodologies, listed in order of preference: a. Written notice to the last known postal address in the records of the individual or entity; b. Telephone Notice; c. Electronic notice; or d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed $50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice. Substitute notice consists of all of the following: i. Email notice if the individual or the entity has email addresses for the members of the affected class of residents; ii. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and iii. Notice to major statewide media.	Agency	
7	In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to section E. of Code of Virginia, §18.2-186.6, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15 U.S.C.§1681(a)(p), of the timing, distribution, and content of the notice.	Agency	
8	Not provide notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advises the individual or entity that the notice would impede a criminal or civil investigation, or homeland security or national security. Notice shall be made without unreasonable delay after the law-enforcement agency determines that the notification will no long impede the investigation or jeopardize national or homeland security.	Agency	
10.2.2 Requirements	Commensurate with sensitivity and risk, each Agency shall or shall require that its service provider document inventory management practices that address the following components, at a minimum:		
1	Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.	Agency	
2	Identify whether personal IT assets are allowed onto premises that house IT systems and data, and if so, identify the controls necessary to protect these IT systems and data.	Agency	
3	Remove data from IT assets prior to disposal in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (COV ITRM Standard SEC514).	Agency and ISP	Agency must inform ISP
4	Require creation and periodic review of a list of agency hardware and software assets.	Agency with ISP	Agency requires and ISP does it

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	**All new requirements are listed in blue and have a compliance data of 1/1/09** **Please note Infrastructure Service Provider (ISP) where applicable**	**Responsibility**	**Comment**
10.3.2 Requirements	Each Agency shall or shall require that its service provider document software license management practices that address the following components, at a minimum:		
1	Require the use only of Agency approved software on IT systems.	Agency with ISP	Agency for agency users ISP for technical staff
2	Assess periodically whether all software is used in accordance with license agreements.	Agency and ISP	Agency for agency software ISP for Infrastructure software
10.4.2 Requirements	Each Agency shall, or shall require that its service provider, document configuration management and change control practices so that changes to the IT environment do not compromise IT security controls.	Agency and ISP	Application: Agency Infrastructure: ISP Input from the agency