

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<p style="text-align: center;"><b>All new requirements are listed in blue and have a compliance data of 1/1/10</b>  <b>Please note Infrastructure Service Provider (ISP) where applicable</b></p>	Responsibility	Comment
1.3	<p><b>Roles and Responsibilities</b>  Each agency should utilize an organization chart that depicts the reporting structure of employees <b>when assigning</b> specific responsibilities for the security of IT systems and data. <b>Each agency shall maintain documentation</b> regarding specific roles and responsibilities relating to information security.</p>	Agency	
1.4	<p><b>Information Security Program</b> Each Agency shall establish, document, implement, and maintain its IT security program appropriate to its business and technology environment in compliance with this <i>Standard</i>. In addition, because resources that can reasonably be committed to protecting IT systems are limited, each Agency must implement its <b>information</b> security program in a manner commensurate with sensitivity and risk.</p>	Agency	
1.5	<p><b>Exceptions to Security Requirements</b>  If an Agency Head determines that compliance with the provisions of this Standard or any related information security standards would adversely impact a business process of the agency, the Agency Head may request approval to deviate from a specific requirement by submitting an exception request to the CISO. For each exception, the requesting agency shall fully document:</p> <ol style="list-style-type: none"> <li>1. The business need,</li> <li>2. The scope and extent,</li> <li>3. Mitigating safeguards,</li> <li>4. Residual risks,</li> <li>5. The specific duration, and</li> <li>6. Agency Head approval.</li> </ol> <p>Each request shall be in writing to the CISO and approved by the Agency Head indicating acceptance of the defined residual risks. Included in each request shall be a statement detailing the reasons for the exception as well as mitigating controls and all residual risks. Requests for exception shall be evaluated and decided upon by the CISO, and the requesting party informed of the action taken. An exception cannot be processed unless all residual risks have been identified and the Agency Head has approved, indicating acceptance of these risks. Denied exception requests may be appealed to the CIO of the Commonwealth. The form that agencies must use</p>	Agency	
1.6	<p><b>Exemptions from Applicability</b> The following are explicitly exempt from complying with the requirements defined in this document:</p> <ol style="list-style-type: none"> <li>1. Systems under development and/or experimental systems that do not create additional risk to production systems.</li> <li>2. Surplus and retired systems.</li> </ol>	Agency	
2.2	<b>Key Information Security Roles and Responsibilities</b>		
2.2.4	<b>Agency Head</b>		
	Each Agency Head is responsible for the security of the agency's IT systems and data. The Agency Head's IT security responsibilities include the following:		

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<p style="text-align: center;"><b>All new requirements are listed in blue and have a compliance data of 1/1/10</b>  <b>Please note Infrastructure Service Provider (ISP) where applicable</b></p>	Responsibility	Comment
1	Designate an Information Security Officer (ISO) for the agency, no less than biennially. Note: Acceptable methods of communicating the designation to the CISO, include: <ul style="list-style-type: none"> <li>• An email directly from the agency head, or</li> <li>• An email from the agency which copies the agency head, or</li> <li>• A hard-copy letter or facsimile transmission signed by the agency head.</li> <li>• This designation must include the following information:               <ol style="list-style-type: none"> <li>a. ISO's name</li> <li>b. ISO's title</li> <li>c. ISO's contact information</li> </ol> </li> </ul>	Agency	
2	Ensure that an agency information security program is maintained, that is sufficient to protect the agency's IT systems, and that is documented and effectively communicated. Managers in all agencies and at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.	Agency	
3	Review and approve the agency's Business Impact Analyses (BIAs), Risk Assessments (RAs), and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.	Agency	
4	Review or have the designated ISO review the System Security Plans for all agency IT systems classified as sensitive, and: <ul style="list-style-type: none"> <li>• <input type="checkbox"/> Approve System Security Plans that provide adequate protections against security risks; or</li> <li>• <input type="checkbox"/> Disapprove System Security Plans that do not provide adequate protections against security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against security risks.</li> </ul>	Agency	
5	Ensure compliance is maintained with the current version of the <i>IT Security Audit Standard</i> (COV ITRM Standard SEC502). This compliance must include, but is not limited to: <ol style="list-style-type: none"> <li>a. Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;</li> <li>b. Requiring that the planned IT security audits are conducted;</li> <li>c. Receiving reports of the results of IT security audits;</li> <li>d. Requiring development of Corrective Action Plans to address findings of IT security audits; and</li> <li>e. Reporting to the CISO all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.</li> </ol>	Agency	
6	Ensure a program of information security safeguards is established.	Agency	
7	Ensure an information security awareness and training program is established.	Agency	
8	Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.	Agency	
9	Identify a System Owner who is generally the Business Owner for each agency sensitive system. Each System Owner shall assign a Data Owner(s), Data Custodian(s) and System Administrator(s) for each agency sensitive IT system.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<p style="text-align: center;"><b>All new requirements are listed in blue and have a compliance data of 1/1/10</b>  <b>Please note Infrastructure Service Provider (ISP) where applicable</b></p>	Responsibility	Comment
10	Prevent or have designee prevent conflict of interests and adhere to the security concept or <a href="#">separation</a> or 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 information 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	
<b>2.2.5</b>	<b>Information Security Officer (ISO)</b>		
	The ISO is responsible for developing and managing the agency's information security program. The ISO's duties are as follows:		
1	Develop and manage an agency information security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.	Agency	
2	Verify and validate that all agency IT systems and data are classified for sensitivity.	Agency	
3	Develop and maintain an information security awareness and training program for agency staff, including contractors and IT service providers. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to any system, and no less than annually, thereafter.	Agency	
4	Implement and maintain the appropriate balance of preventative, detective and corrective controls for agency IT systems commensurate with data sensitivity, risk and systems criticality.	Agency	
5	Mitigate and report all IT security incidents in accordance with §2.2-603 of the Code of Virginia and VITA requirements and take appropriate actions to prevent recurrence.	Agency	
6	Maintain liaison with the CISO.	Agency	
<b>2.2.6</b>	<b>Privacy Officer</b>		
	An agency must have a Privacy Officer if required by law or regulation, such as the Health Insurance Portability and Accountability Act (HIPAA), and may choose to have one where not required. Otherwise, these responsibilities are carried out by the ISO. The Privacy Officer provides guidance on:		
1	The requirements of state and federal Privacy laws.	Agency	
2	Disclosure of and access to sensitive data.	Agency	
3	Security and protection requirements in conjunction with IT systems when there is some overlap among sensitivity, disclosure, privacy, and security issues.	Agency	
<b>2.2.7</b>	<b>System Owner</b>		
	The System Owner is the agency business manager responsible for having an IT system operated and maintained. With respect to IT security, the System Owner's responsibilities include the following:		
1	Require that the IT system users complete any system unique security training prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.	Agency	
2	Manage system risk and developing any additional information security policies and procedures required to protect the system in a manner commensurate with risk.	Agency	
3	Maintain compliance with COV Information Security policies and standards in all IT system activities.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
4	Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system.	Agency	
5	Designate a System Administrator for the system.	Agency	
<b>2.2.8</b>	<b>Data Owner</b>		
	The Data Owner is the agency manager responsible for the policy and practice decisions regarding data, and is responsible for the following:		
1	Evaluate and classify sensitivity of the data.	Agency	
2	Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs.	Agency	
3	Communicate data protection requirements to the System Owner.	Agency	
4	Define requirements for access to the data.	Agency	
<b>2.2.9</b>	<b>System Administrator</b>		
	The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency information security program on IT systems for which the System Administrator has been assigned responsibility.	Agency	
<b>2.2.10</b>	<b>Data Custodian</b>		
	Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:		
1	Protecting the data in their possession from unauthorized access, alteration, destruction, or usage.	Agency	
2	Establishing, monitoring, and operating IT systems in a manner consistent with COV Information Security policies and standards.	Agency	
3	Providing Data Owners with reports, when necessary and applicable.	Agency	
<b>2.2.11</b>	<b>IT System Users</b>		
	All users of COV IT systems including employees and contractors are responsible for the following:		
1	Reading and complying with agency information security program requirements.	Agency	
2	Reporting breaches of IT security, actual or suspected, to their agency management and/or the CISO.	Agency	
3	Taking reasonable and prudent steps to protect the security of IT systems and data to which they have access.	Agency	
<i>2.3.2 Requirements</i>			
	Each Agency <b>should</b> :		
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, if any. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well.	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
5	For each essential business function and dependent function, assess whether the function depends on an IT system to be recovered. Each IT system that is required to recover an essential function or a dependent function shall be considered sensitive relative to availability. For each such system, each agency shall: a. Determine and document the required Recovery Time Objectives (RTO), based on agency and COV goals and objectives. b. Determine and document the Recovery Point Objectives (RPO).	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) and IT System Security Plans (Section 4.2).	Agency	
7	Conduct periodic review and revision of the Agency BIAs, as needed, but at least once every three years.	Agency	
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 reviewed and classified as appropriate 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 all residual risks.	Agency	
9	Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process defined in this Standard.	Agency	
2.5.2 Requirements			
	Each ISO or designated Sensitive System Owner(s) 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	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			

Reference #	Description of Control		
<b>COV IT Security Standard (SEC501-01)</b>	<b>All new requirements are listed in blue and have a compliance data of 1/1/10 Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
	For each IT system classified as sensitive, the data owning agency shall:		
1	Conduct <b>and document</b> a formal RA of the IT system, as needed, but not less than once every three years.	Agency with ISP	ISP provide technical advice
2	Conduct <b>and document</b> 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	
<i>2.7.2 Requirements</i>			
	For each IT system classified as sensitive, the <b>data-owning</b> agency shall:		
1	Require that the IT systems undergo an IT Security Audit as required by and in accordance with <u>the current version of the IT Security Audit Standard</u> (COV ITRM Standard SEC502).	Agency	
2	Assign an individual to be responsible for managing IT Security Audits.	Agency	
<i>3.2.2 Requirements</i>			
	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 ( <b>DR</b> ) planning activities.	Agency	
2	Based on BIA and RA results, develop <b>IT disaster components of the</b> Agency COOP IT-related documentation which identifies: a. Each IT system that is necessary to recover essential business functions or dependent business functions and the Recovery Time Objective (RTO) and Recovery Point Objective (RPO) for each; and b. Personnel contact information and incident notification procedures.	Agency	
3	Require an annual exercise (or more often as necessary) of IT <b>DR</b> components to assess their adequacy and effectiveness.	Agency with ISP Agency with ISP	ISP's notification procedures ISP provide only where IT technical is involved.
4	Require review and revision of IT <b>DR</b> components following the exercise (and at other times as necessary).	Agency with ISP	ISP provide technical assistance.
<i>3.3.2 Requirements</i>			
	Each Agency shall:		
1	Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions <b>and dependent business functions</b> .	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	
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
<i>3.4.2 Requirements</i>			

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
	For every IT system identified as sensitive <b>relative to availability</b> , each Agency shall or shall require that its service provider implement backup and restoration plans to support restoration of systems, data <b>and applications</b> 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
11	<b>Document and exercise a strategy for testing that IT system and data backups are functioning as expected and the data is present in a usable form.</b>	<b>Agency with ISP</b>	<b>ISP provide IT technical advice</b>
12	<b>For systems that are sensitive relative to availability, document and exercise a strategy for testing disaster recovery procedures, in accordance with the agency's Continuity of Operations Plan.</b>	<b>Agency with ISP</b>	<b>ISP provide IT technical advice</b>
<i>4.2.2 Requirements</i>			
	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 <b>and planned</b> 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	
3	Plan, document, <b>and implement</b> additional <b>security</b> 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 ( <b>i.e., due to material change</b> ), 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
<i>4.3.2 Requirements</i>			
	Each Agency shall or shall require that its service provider:		
1	Identify, document, and apply appropriate baseline security configurations to <b>all</b> Agency IT systems, regardless of their sensitivity.	Agency with ISP	Application: Agency Infrastructure: ISP

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
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	Monitor systems for security baselines and policy compliance.	ISP	
5	Review and revise all security configuration standards annually, or more frequently, as needed.	ISP	
6	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
7	Require periodic <b>operating system level</b> vulnerability scanning of <b>sensitive</b> IT systems in a <b>frequency</b> commensurate with sensitivity and risk, to <b>assess</b> whether security configurations are in place and if they are functioning effectively.	Agency with ISP	Agency responsible for application scanning
8	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	
<b>4.4.2 Requirements</b>			
	For every sensitive Agency IT system <b>that shares data with non-Commonwealth entities</b> , the Agency shall require or shall specify that its service provider require:		
1	The System Owner, in consultation with the Data Owner, <b>shall</b> document IT systems with which data is shared. This documentation <b>must</b> include: a. The types of shared data; b. The direction(s) of data flow; and 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 <b>shall</b> develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.	Agency	
3	The System Owners of the IT systems that share data <b>shall</b> inform one another regarding other IT systems with which their IT systems interconnect or share data, and <b>shall</b> inform one another prior to establishing any additional interconnections or data sharing.	Agency	
4	The written <b>agreement shall specify</b> 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 <b>by</b> any legal requirements ( <b>i.e., HIPAA</b> ) regarding handling, protection, and disclosure of the shared data.	Agency	
6	The written agreement <b>shall specify</b> each Data Owner's authority to approve access to the shared data.	Agency	
7	The System Owners <b>shall</b> approve and enforce the agreement.	Agency	
<b>4.5.2 Requirements</b>			
	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

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
3	Provide malicious program detection, protection, eradication, logging, and reporting capabilities.	ISP	
4	Provide malicious code protection mechanisms <a href="#">via</a> multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms. <del>Provide protection against malicious program through the use of mechanisms that:</del>	ISP	
5	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	
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
<b>4.6.2 Requirements</b>			
	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	
	<b><u>Project Initiation</u></b>		
2	Perform an initial risk analysis based on <a href="#">the known requirements</a> 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 <a href="#">IT System and Data Sensitivity Classification</a> ) that the IT system will process and the sensitivity of <a href="#">the</a> proposed IT system.	Agency	

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
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 <a href="#">IT System Security Plans</a> ) 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.
	<b><u>Project Definition</u></b>		
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 with ISP	ISP technical assistance on proposed infrastructure.
8	Verify that the IT system development process designs, develops, and implements IT security controls that meet <a href="#">information</a> security requirements in the design specifications.	Agency with ISP	ISP technical assistance on proposed infrastructure.
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 with ISP	ISP technical assistance on proposed infrastructure.
	<b><u>Implementation</u></b>		
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 <a href="#">Risk Assessment</a> (see <a href="#">Risk Assessment</a> ) 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 <a href="#">this Standard</a> .	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 <a href="#">information</a> security risks, and comply with the other requirements (see <a href="#">IT Systems Security Plans</a> ) of this document.	Agency with ISP	ISP technical assistance on proposed infrastructure.
	<b><u>Disposition</u></b>		
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 (see <a href="#">Data Storage Media Protection</a> ), 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 <i>current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard</i> (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 <a href="#">documented and</a> followed:		
	<b><u>Application Planning</u></b>		
1	Data_Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.	Agency	
2	Risk Assessment – If the data classification identifies the system as sensitive, a risk assessment shall be <a href="#">conducted before</a> development begins and after planning is complete.	Agency	

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
3	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	
4	Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. <b>When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:</b> a. <b>Encrypted communication channels shall be established for the transmission of sensitive information;</b> b. <b>Sensitive information shall not be visibly transmitted between the client and the application; and</b> c. <b>Sensitive information shall not be stored in hidden fields that are part of the application interface.</b>	Agency and ISP Agency and ISP Agency	Agency for agency controlled devices ISP for ISP controlled devices Agency for agency controlled devices ISP for ISP controlled devices
	<b><u>Application Development</u></b>		
	The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.	Agency	
5	<b>Authentication – Application-based authentication and authorization shall be performed for access to data that is available through the application but is not considered publicly accessible.</b>	Agency	
6	<b>Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.</b>	Agency	
7	<b>Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).</b>	Agency	
8	<b>Input Validation – All application input shall be validated irrespective of source.</b> Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.	Agency	
9	<b>Default Deny – Application access control shall implement a default deny policy, with access explicitly granted</b>	Agency	
10	<b>Principle of Least Privilege – All processing shall be performed with the least set of privileges required.</b>	Agency	
11	<b>Quality Assurance – Internal testing shall include at least one of the following: penetration testing, fuzz testing, or a source code auditing technique. Third party source code auditing and/or penetration testing should be conducted commensurate with sensitivity and risk.</b>	Agency	
12	<b>Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
	<b><u>Production and Maintenance</u></b>		
13	<b>Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
14	<b>Internet-facing applications classified as sensitive shall have periodic vulnerability scans run against the applications and supporting server infrastructure, and always when any significant change to the environment or application has been made. Any remotely exploitable vulnerability shall be remediated immediately. Other vulnerabilities should be remediated without undue delay.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
4.8.2 Requirements			

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<p style="text-align: center;"><b>All new requirements are listed in blue and have a compliance data of 1/1/10</b>  <b>Please note Infrastructure Service Provider (ISP) where applicable</b></p>	Responsibility	Comment
	Each agency ISO is accountable for ensuring the following steps are followed and documented:		
	<b><u>Wireless LAN (WLAN) Connectivity on the COV Network</u></b>		
1	<p>The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.</p> <ul style="list-style-type: none"> <li>a. Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);</li> <li>b. WLAN infrastructure must authenticate client devices prior to permitting access to the WLAN;</li> <li>c. LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;</li> <li>d. Only COV owned or leased equipment shall be granted access to an internal WLAN;</li> <li>e. All WLAN communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption protocols ( i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);</li> <li>f. Physical or logical separation between WLAN and wired LAN segments must exist;</li> <li>g. All COV WLAN access and traffic must be monitored for malicious activity, and associated</li> </ul>	ISP	
	<b><u>WLAN Hotspot (Wireless Internet)</u></b>		
2	<p>When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:</p> <ul style="list-style-type: none"> <li>a. WLAN Hotspots must have logical or physical separation from the agency's LAN;</li> <li>b. WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;</li> <li>c. All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and</li> <li>d. Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.</li> </ul>	ISP	
	<b><u>Wireless Bridging</u></b>		
3	<p>The following network configuration shall be used when bridging two wired LANs:</p> <ul style="list-style-type: none"> <li>a. All wireless bridge communications must utilize a secure encryption algorithm that provides an automated mechanism to change the encryption keys multiple times during the connected session and provide support for secure encryption methods (i.e., the Counter Mode with Cipher Block Chaining Message Authentication Code Protocol encryption mechanism based on the Advanced Encryption Standard cipher);</li> <li>b. Wireless bridging devices will not have a default gateway configured;</li> <li>c. Wireless bridging devices must be physically or logically separated from other networks;</li> <li>d. Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;</li> <li>e. Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and</li> <li>f. Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).</li> </ul>	ISP	
5.2.2 Requirements			

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
	Each Agency shall or shall require that its service provider document <b>and implement</b> formal account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:		
	<b>For all internal and external IT systems:</b>		
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.	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
4	<b>If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access that:</b> 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	<b>Review all user accounts for the user's continued need to access all IT systems.</b>	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	<b>If the IT system is classified as sensitive, prohibit the use of guest accounts.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
9	<b>Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
10	<b>Prohibit the display of the last logon user ID on multi-user systems. Desktop and laptop systems assigned to a specific user are exempt from this requirement.</b>	Agency and ISP	Application: Agency Infrastructure: ISP
11	Lock an account automatically if it is not used for a predefined period.	Agency and ISP	Application: Agency Infrastructure: ISP
12	Disable unneeded accounts.	Agency and ISP	Application: Agency Infrastructure: ISP
13	Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.	Agency and ISP	Application: Agency Infrastructure: ISP
14	Associate access levels with group membership, where <b>practicable</b> , 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

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
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	Prohibit the granting of local administrator rights to users. An Agency Head may grant exceptions to this requirement for those employees whose documented job duties are primarily the development and/or support of IT applications and infrastructure. These exception approvals must be documented annually and include the Agency Head's explicit acceptance of defined residual risks.	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
	<b>For all internal IT systems:</b>		
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 confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner or designee to establish accounts for all sensitive IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
22	Require secure delivery of access credentials to the user based on information already on file.	Agency and ISP	Application: Agency Infrastructure: ISP
23	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
24	Promptly remove access when no longer required.	Agency and ISP	Application: Agency Infrastructure: ISP
	<b>For all external IT systems:</b>		
25	Require secure delivery of access credentials to users of all external IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
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 all sensitive external IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
27	Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).	Agency	
	<b>For all service and hardware accounts</b>		
28	Document account management practices for all agency created service accounts, including, but not limited to granting, administering and terminating accounts.	Agency and ISP	Application: Agency Infrastructure: ISP
5.3.2 Requirements			

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
	Each agency shall or shall require that its service provider document <b>and implement</b> 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 <b>pin number with a minimum of 4 digits</b> .	Agency and ISP	Application: Agency Infrastructure: ISP
3	Require password complexity: a. At least eight characters in length, <b>and</b> b. Utilize at least three of the following four: 1) Special characters, 2) Alphabetical characters, 3) Numerical characters, 4) 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 <b>all sensitive</b> IT systems to allow users to change their password at <b>most, once per 24 hour period</b> .	Agency and ISP	Application: Agency Infrastructure: ISP
8	Require users of <b>all sensitive</b> 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 <b>they suspect</b> their passwords have been compromised.	Agency and ISP	Application: Agency Infrastructure: ISP
10	<b>Configure all sensitive IT systems to maintain_at least</b> the last 24 passwords used in the password history files to prevent the reuse <b>of the</b> 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 <b>account</b> of <b>sensitive</b> 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 for technical staff      ISP
12	<b>For sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner.</b>	<b>Agency and ISP</b>	<b>Agency for agency users for technical staff      ISP</b>
13	Require that forgotten initial passwords be replaced rather than reissued.	Agency and ISP	Agency for agency users for technical staff      ISP
14	Shared passwords <b>shall not be used</b> on <b>any</b> IT systems.	Agency and ISP	Application: Agency Infrastructure: ISP
15	Prohibit the storage_of passwords in clear text.	Agency and ISP	Application: Agency Infrastructure: ISP
16	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)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
17	Suppress the display of passwords on the screen as they are entered.	Agency and ISP	Application: Agency Infrastructure: ISP
18	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
19	Require passwords to be set on device management user interfaces for all network connected devices.	ISP	
20	Document and store hardware passwords securely.	ISP	
21	Implement procedures to handle lost or compromised passwords and/or tokens.	Agency and ISP	Application: Agency Infrastructure: ISP
22	Set an account lockout threshold of not greater than 10 invalid attempts and the lockout duration for at least 15 minutes.	Agency and ISP	Application: Agency Infrastructure: ISP
5.4.2 Requirements			
	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 agency 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
7	Where supported by features of the system, session timeouts shall be implemented after a period of not longer than 30 minutes of inactivity and less, commensurate with sensitivity and risk. Where not supported by features of the system, mitigating controls must be implemented.	Agency with ISP	Agency: Policy ISP: Technical solution
6.2.2 Requirements			
	Each Agency shall or shall require that its service provider document and implement 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
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 accepting all residual risks. the exception shall include 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 residual risks.	Agency and ISP	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
3	Prohibit the storage of any Commonwealth data on non-COV issued computing devices. This prohibition, at the agency's discretion need not apply to Internet-facing web sites serving non-sensitive data. Agency contactors may store non-sensitive COV data for the execution of the agency contract. This requirement is due to records retention and Freedom of Information Act (FOIA) complexities, as well as the associated information security risks.	Agency and ISP	
4	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
5	Prohibit the connection of any non-COV owned data storage media or device to a COV-owned resource, unless connecting to a guest network or guest resources. This prohibition, at the agency's discretion need not apply to an approved vendor providing operational IT support services under contract.	Agency and ISP	
6	Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing residual risk approved in writing by the Agency Head.	Agency and ISP	
7	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
8	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 sensitive as related to confidentiality. 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
9	Implement processes to sanitize data storage media prior to disposal or reuse.	Agency and ISP	Agency controlled data ISP controlled data
	<b>6.3.2 If encryption is in use for the Agency</b>		
6.3.2 Requirements			
	Commensurate with sensitivity and risk, each Agency or their service provider 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
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 encryption 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 controlled data ISP controlled data
3	Require encryption for the transmission of data that is sensitive relative to confidentiality or integrity over non-Commonwealth networks or any publicly accessible networks, or any transmission outside of the data's broadcast domain; however, digital signatures may be utilized for data that is sensitive solely relative to integrity.	Agency and ISP	Agency controlled data ISP controlled data
6.4.2			
	<b>Recommended Best Practices</b>		
	These recommendations apply to non-electronic media:		

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
1	While in use, limit access based on a need to know basis by physically controlling access. For example, sensitive documents printed to a global printer should be retrieved without delay.	Agency and ISP	Agency controlled data ISP controlled data
2	While not in use, store in a secure location with appropriate physical controls.	Agency and ISP	Agency controlled data ISP controlled data
3	When no longer needed, securely destroy using appropriate destruction methods such as erasing white or black boards and shredding paper.	Agency and ISP	Agency controlled data ISP controlled data
7.2 Requirements			
	Each agency shall or shall require that its service provider document and implement facilities security practices. At a minimum, these practices must include the following components:		
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, commensurate with risk, to protect against human, natural, and environmental threats.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
3	Require appropriate environmental controls such as electric power, heating, fire suppression, humidity control, 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 or designee 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 and implement 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 from facility areas that house sensitive IT systems or data.	Agency and ISP	Agency for agency locations ISP for CESC and SWESC
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

Reference #	Description of Control	Responsibility	Comment
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>		
6	Temporarily disable physical and logical access rights when personnel <b>do not need such access for a prolonged period in excess of 30 days because they are not working</b> 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 <b>separation</b> 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 <b>separation</b> 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 ISO shall:		
1	Include any Agency-specific <b>information security</b> training requirements in the Agency <b>information security</b> awareness and training program.	Agency	
2	<b>Require that all IT system users, including employees and contractors, receive IT security awareness training annually, or more often as necessary. Generally, best practice is that annual security awareness training lasts at least one hour.</b>	Agency and ISP	Agency for agency users ISP for technical staff
3	<b>Require</b> additional role-based <b>information security</b> 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
4	Implement processes to monitor and track completion of <b>information security</b> training.	Agency and ISP	Agency for agency users ISP for technical staff
5	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
6	Develop an <b>information security</b> 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 <b>separation</b> of duties; c. Prevention and detection of <b>information security</b> incidents, including those caused by malicious code; d. Proper disposal of data storage media; e. <b>Proper use of encryption</b> ; f. Access controls, including creating and changing passwords and the need to keep them confidential; g. <b>Agency acceptable use policies</b> ; h. Agency Remote Access policies; and i. Intellectual property rights, including software licensing and copyright issues. j. <b>Responsibility for the security of COV data</b> ; k. <b>Phishing</b> ; and l. <b>Social engineering</b> .	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
7	Require documentation of IT system users' acceptance of the agency's security policies after receiving <a href="#">information security</a> training.	Agency	
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 (DHRM) 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	<a href="#">Direct the proper use of encryption for transmitting sensitive data.</a>	Agency and ISP	Agency for agency users ISP for technical staff
3	<a href="#">Direct the use of an agency authorized COV warning banner to communicate that IT systems and their use may be monitored and viewed by authorized personnel; and there is no expectation of privacy when using a Commonwealth IT system.</a>	Agency and ISP	Agency for agency users ISP for technical staff
4	<a href="#">Require acknowledgement that monitoring of IT systems and data may include, but is not limited to, network traffic; application and data access; keystrokes (only when required for security investigations and approved in writing by the Agency Head); and user commands; email and Internet usage; and message and data content.</a>	Agency and ISP	Agency for agency users ISP for technical staff
5	<a href="#">Prohibit users from:</a> a. Installing or using proprietary encryption hardware/software on <a href="#">Commonwealth</a> systems; b. Tampering with security controls configured on <a href="#">COV</a> workstations; c. Installing personal software on a <a href="#">Commonwealth</a> system; d. <a href="#">Adding hardware to, removing hardware from, or modifying hardware on a COV system; and</a> e. <a href="#">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).</a>	Agency and ISP	Agency for agency users ISP for technical staff and provide technical advice
6	Prohibit the <a href="#">storage, use or transmission</a> of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with <a href="#">licensing and copyright laws</a> governing the materials.	Agency and ISP	Agency for agency users ISP for technical staff
7	<a href="#">When connected to internal networks from COV guest networks or non-COV networks, data transmission shall only use full tunneling and not use split tunneling.</a>	Agency and ISP	Agency for agency users ISP for technical staff
8	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
8.5.2 Requirement			
	Each agency shall:		
1	<a href="#">Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality or integrity; however, digital signatures may be utilized for data that is sensitive solely relative to integrity as stated in the encryption component of this Standard. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.</a>	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	Responsibility	Comment
2	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.	Agency	
	The following text is an example of an email disclaimer for consideration when meeting with your agency's legal counsel.		
	<i>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).</i>  <i>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.</i>		
9.2.2 Requirement			
	Each Agency shall or shall require that its service provider document and implement threat detection practices that at a minimum include the following:		
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	Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).	Agency with ISP	Infrastructure
3	Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.	ISP	Infrastructure
4	Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.	Agency with ISP	Infrastructure
5	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			
	Each agency shall, or shall require that its service provider, document and implement information security monitoring and logging practices that include the following components, at a minimum:		
1	Designate individuals responsible for the development and implementation of information 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. At a minimum, logs will include: a. The event; b. The user ID associated with the event; and c. The time the event occurred.	Agency and ISP	Application: Agency Infrastructure: ISP
3	Routinely 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 installation or use of unauthorized monitoring devices.	Agency and ISP	Application: Agency Infrastructure: ISP

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<b>All new requirements are listed in blue and have a compliance data of 1/1/10</b> <b>Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
6	Prohibit the use of keystroke logging, except when required for security investigations and a documented business case outlining the need and residual risk has been approved in writing by the Agency Head.	Agency and ISP	Application: Agency Infrastructure: ISP
9.4.2 Requirements			
	Each agency shall document information security incident handling practices and where appropriate the agency shall incorporate its service provider's procedures for incident handling practices that include the following at a minimum:		
1	Designate an Information 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 and zero-day exploits.	Agency and ISP	
4	Establish information security incident categorization and prioritization based on the immediate and potential adverse effect of the information security incident and the sensitivity of affected IT systems and data.	Agency and ISP	
5	Identify immediate mitigation procedures, including specific instructions, based on information 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. All COV agencies are encouraged to report security incidents; however, 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 information security incident recording and reporting requirements, including a template for the incident report.	Agency	
8	Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.	Agency and ISP	ISP Technical assistance
9	Report information security incidents only through channels that have not been compromised.	Agency	
9.5.2 Requirements			
	All of the following are industry best practices. Where electronic records or IT infrastructure are involved, the following are requirements that each agency shall adhere to. Based on their business requirements, some agencies may need to comply with regulatory and/or industry requirements that are more restrictive. Where non-electronic records are involved or implied, the following are advisory in nature, but are strongly recommended: Each agency shall:		

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	<p style="text-align: center;"><b>All new requirements are listed in blue and have a compliance data of 1/1/10</b>  <b>Please note Infrastructure Service Provider (ISP) where applicable</b></p>	Responsibility	Comment
1	<p>Identify <b>and document</b> all agency systems, processes, and logical <del>and</del> <b>or</b> 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.</p> <p>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.</p> <p><u>"Redact" means alteration or truncation of data such that no more than the following are accessible as part of the information:</u>  <u>a. Five digits of a social security number; or</u>  <u>b. The last four digits of a driver's license number, state identification card number, or account number.</u></p>	Agency with ISP	
2	<p>Include provisions in any third party contracts requiring that the third party and third party subcontractors:</p> <p>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.</p>	Agency	
3	<p>redacted Personal Information by any mechanism, including, but not limited to:</p> <p>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.</p> <p>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.</p> <p>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.</p> <p>The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #7, below.</p>	Agency	
4	<p>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. Agencies shall notify the CISO when notification of affected individuals has been completed.</p>	Agency	

Reference #	Description of Control		
COV IT Security Standard (SEC501-01)	All new requirements are listed in blue and have a compliance data of 1/1/10 Please note Infrastructure Service Provider (ISP) where applicable	Responsibility	Comment
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	
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: 1) Email notice if the individual or the entity has email addresses for the members of the affected class of residents; 2) Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and 3) Notice to major statewide media.	Agency	
7	Hold the release of 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 and implement 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 <u>current version of the Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (COV_ITRM Standard SEC514)</u> .	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		
<b>COV IT Security Standard (SEC501-01)</b>	<b>All new requirements are listed in blue and have a compliance data of 1/1/10 Please note Infrastructure Service Provider (ISP) where applicable</b>	<b>Responsibility</b>	<b>Comment</b>
<i>10.3.2 Requirements</i>			
	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 of <b>only agency approved software and service provider approved systems management software</b> 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
<i>10.4.2 Requirements</i>			
	Each Agency shall, or shall require that its service provider, document <b>and implement</b> configuration management and change control practices so that changes to the IT environment do not compromise <b>security</b> controls.	Agency and ISP	Application: Agency Infrastructure: ISP with input from the agency