VIRGINIA DEPARTMENT OF MOTOR VEHICLES

IT SECURITY POLICY

Version 2.4
September 19, 2012

Approval

Douglas G. Mack	Dave Burhop	for Richard D. Holcomb
Douglas G. Mack IT Security Director ISO	Dave Burhop Deputy Commissioner CIO	Richard D. Holcomb Commissioner Agency Head
8/24/2012	8-29-12	9-19-2012
Date	Date	Date

Revision History

Version	Date	Purpose of Revision
2.0		Base Document
2.1	07/23/2012	Draft 1 – Given to ISO for Review
2.2	08/15/2012	Draft 2 – Incorporates Changes from ISO – Given to ISO for Review
2.3	08/27/2012	Draft 3 – Incorporates Changes from ISO – Given to CIO for Review
2.4	09/19/2012	APPROVED

Table of Contents

Sheet No. - No. of Pages

AU-2 | AUDITABLE EVENTS
AU-3 | CONTENT OF AUDIT RECORDS
AU-4 | AUDIT STORAGE CAPACITY
AU-5 | RESPONSE TO AUDIT PROCESSING FAILURES
AU-6 | AUDIT REVIEW, ANALYSIS, AND REPORTING
AU-8 | TIME STAMPS
AU-9 | PROTECTION OF AUDIT INFORMATION
AU-11 | AUDIT RECORD RETENTION
AU-12 | AUDIT GENERATION
CA-2 | SECURITY ASSESSMENTS
CA-3 | INFORMATION SYSTEM CONNECTIONS
CA-3-COV | INFORMATION SYSTEM CONNECTIONS (COV)
CA-6 | SECURITY AUTHORIZATION
CA-7 | CONTINUOUS MONITORING
CM-2 | BASELINE CONFIGURATION
CM-2-COV | BASELINE CONFIGURATION (COV)
CM-3 | CONFIGURATION CHANGE CONTROL
CM-3-COV | CONFIGURATION CHANGE CONTROL (COV)
CM-4 | SECURITY IMPACT ANALYSIS
CM-5 | ACCESS RESTRICTIONS FOR CHANGE
CM-6 | CONFIGURATION SETTINGS
CM-7 | LEAST FUNCTIONALITY
CM-8 | INFORMATION SYSTEM COMPONENT INVENTORY
CM-9 | CONFIGURATION MANAGEMENT PLAN
CP-2 | CONTINGENCY PLAN
CP-3 | CONTINGENCY TRAINING
CP-4 | CONTINGENCY PLAN TESTING AND EXERCISES
CP-6 | ALTERNATE STORAGE SITE
CP-7 | ALTERNATE PROCESSING SITE
CP-8 | TELECOMMUNICATIONS SERVICES
CP-9 | INFORMATION SYSTEM BACKUP
CP-10 | INFORMATION SYSTEM RECOVERY AND RECONSTITUTION
IA-2 | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)
IA-4 | IDENTIFIER MANAGEMENT
IA-5 | AUTHENTICATOR MANAGEMENT
IA-6 | AUTHENTICATOR FEEDBACK
IA-7 | CRYPTOGRAPHIC MODULE AUTHENTICATION
IA-8 | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)
IR-1-COV | INCIDENT RESPONSE (COV)
IR-2 | INCIDENT RESPONSE TRAINING
IR-3 | INCIDENT RESPONSE TESTING AND EXERCISES
IR-4 | INCIDENT HANDLING
IR-4-COV | INCIDENT HANDLING (COV)
IR-4-COV-2 | INCIDENT HANDLING (COV-2)
IR-5 | INCIDENT MONITORING
IR-5-COV | INCIDENT MONITORING (COV)
IR-6 | INCIDENT REPORTING
IR-6-COV | INCIDENT REPORTING (COV)

IR-7 | INCIDENT RESPONSE ASSISTANCE
IR-8 | INCIDENT RESPONSE PLAN
MA-2 | CONTROLLED MAINTENANCE
MA-5 | MAINTENANCE PERSONNEL
MP-2 | MEDIA ACCESS
MP-3 | MEDIA MARKING
MP-4 | MEDIA STORAGE
MP-5 | MEDIA TRANSPORT
MP-6 | MEDIA SANITIZATION
MP-6-COV | MEDIA SANITIZATION (COV)
PE-1-COV | PHYSICAL AND ENVIRONMENTAL PROTECTION (COV)
PE-2 | PHYSICAL ACCESS AUTHORIZATIONS
PE-3 | PHYSICAL ACCESS CONTROL
PE-4 | ACCESS CONTROL FOR TRANSMISSION MEDIUM
PE-5 | ACCESS CONTROL FOR OUTPUT DEVICES
PE-6 | MONITORING PHYSICAL ACCESS
PE-7 | VISITOR CONTROL
PE-8 | ACCESS RECORDS (VISITOR)
PE-9 | POWER EQUIPMENT AND POWER CABLING
PE-10 | EMERGENCY SHUTOFF
PE-11 | EMERGENCY POWER
PE-13 | FIRE PROTECTION
PE-14 | TEMPERATURE AND HUMIDITY CONTROLS
PE-15 | WATER DAMAGE PROTECTION
PE-18 | LOCATION OF INFORMATION SYSTEM COMPONENTS
PL-2 | SYSTEM SECURITY PLAN
PL-2-COV | SYSTEM SECURITY PLAN (COV)
PL-4 | RULES OF BEHAVIOR
PL-4-COV | RULES OF BEHAVIOR (COV)
PL-6 | SECURITY-RELATED ACTIVITY PLANNING
PS-2 | POSITION CATEGORIZATION
PS-3 | PERSONNEL SCREENING
PS-4 | PERSONNEL TERMINATION
PS-5 | PERSONNEL TRANSFER
PS-6 | ACCESS AGREEMENTS
PS-7 | THIRD-PARTY PERSONNEL SECURITY
RA-2 | SECURITY CATEGORIZATION
RA-3 | RISK ASSESSMENT
RA-5 | VULNERABILITY SCANNING
RA-5-COV | VULNERABILITY SCANNING (COV)
SA-2 | ALLOCATION OF RESOURCES
SA-3 | LIFE CYCLE SUPPORT
SA-3-COV-1 | LIFE CYCLE SUPPORT (COV-1)
SA-3-COV-2 | LIFE CYCLE SUPPORT (COV-2)
SA-4 | ACQUISITIONS
SA-5 | INFORMATION SYSTEM DOCUMENTATION
SA-6 | SOFTWARE USAGE RESTRICTIONS
SA-6-COV | SOFTWARE USAGE RESTRICTIONS (COV)

DMV Information Security Policy

Based on VITA SEC501-07 and NIST SP800-53 r4 drafts

Section	Section Names and Content	Comments
1.0	**Introduction**	
1.1	Overview	
1.1	As an agency of the Commonwealth of Virginia (“The Commonwealth”, “COV”), the Virginia Department of Motor Vehicles (“DMV” or “The Agency”) is required by statute, regulation, and policy to implement a comprehensive Information Security (IS) Policy ("IS Policy" or "Policy"). The Agency's Information Security Policy intends to protect the confidentiality, integrity, and availability of information captured, stored, processed, transmitted or otherwise handled by DMV personnel, Agency systems or third-parties working on DMV's behalf. DMV relies on information technology (IT) to effectively deliver government services. Rapid advances in technology and business processes have increased DMV's dependence on IT. DMV information, software, hardware, and telecommunications are important resources and must be protected; the agency IS Policy defines policies and procedures to implement protective measures. DMV is responsible to protect Information that may be in any format, digital or non-digital; these include paper, microfiche/film, whiteboards, flipcharts, audio/video or any other media that may hold data. The Agency is obligated to implement appropriate protections based on content, not format. Information security shall be a team effort with all DMV personnel, including employees, contractors, consultants and vendors, playing an important role. The Agency's policy is that each individual is responsible and accountable for protecting all information entrusted to them and to DMV. Complying with this Information Security Policy and the processes it defines is mandatory for all the personnel who use Agency IT systems or handle Agency information in any capacity.	
1.2	Review	
1.2	The IT Security Director shall review these policies annually, based on their approval date, then provide confirmation to the Commissioner, Chief Information Officer (CIO), and Director of Internal Audit.	
1.3	Policy/Legal Conflicts	
1.3	DMV's Information Security Policy was written to meet or exceed the protections found in existing laws and regulations; any portion of this Policy believed to be in conflict with these directives must be promptly reported to the IT Security Director. In case of conflict between DMV's IS Policy and existing laws or regulations, this order of precedence shall be used to resolve it: 1. Federal/State law which takes precedence over 2. COV Information Security Policy, Standards, Guidelines which takes precedence over 3. DMV Information Security Policy which takes precedence over 4. Any other DMV policies that address any security requirements or controls documented in this Policy **NOTES:** - In cases where DMV's IS policy requirements are more restrictive then either 1. or 2. above, it shall take precedence - Information regarding credit or debit cards, and the systems used to capture, process, store or transmit Cardholder or transaction data presents a special case where Payment Card Industry (PCI) regulations would be overruled by Federal or State laws but would take precedence over COV Policy, Standards & Guidelines.	
1.4	Security Policy Exceptions	
1.4	In rare circumstances, exceptions to this Policy and its guidance may be necessary. The IT Security Director, or authorized designee, must approve all such deviations in writing. A business case for non-compliance must be established and the request for exemption must be approved in advance through a risk management process. This process requires approval by the System Owner, Data Owner (if applicable), and IT Security Director. Depending on the nature of the exception, the security exception procedure documented in the current VITA ITRM SEC501*Information Security Standard* may be required in addition to the Agency's process.	

1.5	Security Policy Compliance & Enforcement	
1.5	Classified employees may be subject to disciplinary action up to and including discharge, under the Commonwealth's Standards of Conduct (DHRM 1.60); wage employees, contractors and consultants assigned to or working for the Agency may be subject to administrative and contractual sanctions. Criminal or civil action may be initiated in appropriate instances. Selective enforcement or non-enforcement of any policy provisions shall not permit non-compliance by any parties covered by the scope of these policies. All suspected or known violations of the law shall be immediately reported to DMV Assistant Commissioner, Enforcement and Compliance.	
1.6	Authorities	
1.6	**Code of Virginia** - § 2.2-603. Authority of Agency Directors - § 2.2-2005. Creation of the Virginia Information Technologies Agency ("VITA"); Appointment of Chief Information Officer (CIO) - § 2.2-2007. Powers of the CIO - §2.2-2009. Additional Powers of the CIO relating to security - § 2.2-2699.5. Information Technology Advisory Council - § 2.2-2817.1. State agencies to establish alternative work schedules, including Telecommuting - §2.2-2827. Restrictions on State employee access to information Infrastructure - §2.2-3803. Administration of systems including personal information; Internet privacy policy - §18.2-186.6. Breach of personal information notification - § 2.2-1124. Disposition of surplus materials	
1.6	**VITA Information Technology Resource Management** • Information Security Policy o IT Information Security Policy (SEC 519-00) (07/24/2009) • Information Security Standards o IT Information Security Standard (SEC501-06) (04/04/2011) o IT Security Audit Standard (SEC502-02) (12/05/2011) o IT Standard Use of Non-Commonwealth Computing Devices to Telework (SEC511-00) (07/01/2007) o Removal of Commonwealth Data from Electronic Media Standard (SEC514-03) (03/15/2008) o Secure Remote Access to Online Court Documents Standard (SEC503-02) (03/28/2005) o Virginia Real Property Electronic Recording Standard (SEC505-00) (05/01/2007) • Information Security Guidelines o Information Systems Facilities Security Guideline (SEC517-00) (04/27/09) o IT Contingency Planning Guideline (SEC508-00) (4/18/07) o IT Data Protection Guideline (SEC507-00) (7/02/07) o IT Logical Access Control Guideline (SEC509-00) (4/18/07) o IT Personnel Security Guideline (SEC513-00) (2/15/2008) o IT Risk Management Guideline (SEC506-01) (12/11/2006) - IT Risk Assessment Instructions- Appendix D (SEC506-01) (12/14/2006) o IT Security Audit Guideline (SEC512-00) (12/20/2007) o IT Security Threat Management Guideline (SEC510-00) (07/01/2007) o IT Systems Asset Management Guideline (SEC518-00) (04/27/09) o IT Systems Security Guideline (SEC515-00) (07/17/2008)	

1.7	Freedom of Information (FOIA)	
1.7	It is the policy of DMV to fully comply with Virginia's Freedom of Information Act. The Virginia Freedom of Information Act (FOIA), located at §2.2-3700 et. seq. of the Code of Virginia, guarantees citizens of the Commonwealth and representatives of the media access to certain public records held by public bodies, public officials, and public employees. A public record is any writing or recording - regardless of whether it is a paper record, an electronic file, an audio or video recording, or any other format - that is prepared or owned by, or in the possession of a public body or its officers, employees or agents in the transaction of public business. All public records are presumed to be open, and may only be withheld if a specific, statutory exemption applies. The release of information by DMV is also governed by the Federal Driver's Privacy Protection Act (18 USC §§ 2721 - 2725) and by Va. Code §§ 46.2-208 through 213. These statutes prohibit DMV from disclosing personal, driver, and vehicle information collected by it in the administration of the motor vehicle laws of Virginia, unless the release of such information meets one of the conditions specified in Va. Code §§ 46.2-208 through 213 and applicable fees are paid.	
1.8	Version Control	
1.8	It is the user's responsibility to ensure they have the latest version of this Policy. The IT Security Director (ISO) distributes all revisions of Information Security policies and procedures to Agency management as they are approved; the current versions are also posted on myDMV on the "Information Security Policies" page: http://intranet/intranet/manuals/istoc.shtml This posted, current version supersedes all others. If you are unable to access DMV's Intranet or have questions regarding this or any other Information Security policy or procedure, please contact the IT Security Director or the IT Security Office.	
2.0	**Information Security Policy Implementation**	
2.1	Purpose	
2.1	This Policy implements the DMV Information Security Program per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the governance, implementation, roles and responsibilities, standards, guidelines, enforcement, review and procedures to appropriately secure the Agency's information and systems.	
2.2	Scope	
2.2	These policies apply to all personnel and locations of the Virginia Department of Motor Vehicles, including employees, contractors, consultants, vendors and any other personnel with access to DMV information, IT systems or networks. NOTE: Any exceptions to this scope shall be described in the applicable policy.	
2.3	Policy Development and Direction	
2.3	The IT Security Director shall develop and administer DMV's Information Security Policy under the direction of the Deputy Commissioner/CIO. The IT Security Director, to the fullest extent of the position's authority, ensures DMV information, systems and networks in all environments are properly secured, and that policies, procedures and standards are enforced for internal and external users. The IT Security Director does not implement technical solutions or controls, but establishes the policies, standards, guidelines and processes needed to accomplish DMV security objectives. Most technical controls are implemented by VITA and the Information Technology Partnership ("ITP" or "Partnership").	
2.4	Management Commitment to Security	
2.4	Management shall ensure that information security within their departments is treated as a regular business problem to be faced and solved, and they are responsible for promoting security as everyone's responsibility. Managers in all administrations, at all locations and at all levels of supervisory responsibility shall provide for the information security needs in areas under their authority. They shall take all reasonable actions to provide adequate information security as mandated by this Policy and to promptly escalate any security-related issues to the IT Security Director.	
2.5	Information Security Resources	
2.5	The Commissioner shall allocate sufficient resources and staff attention to implement information security controls appropriate for securing the information DMV is responsible to protect.	

2.6	Coordination Between Organizational Units	
2.6	Internal and external groups must coordinate effectively to adequately secure DMV's information, IT systems and network. This includes but is not limited to employees, contractors, consultants and vendors. All individuals with a role in developing, implementing or maintaining security controls shall cooperate to the best of their ability to ensure the Agency's information resources are appropriately protected. In addition, all System Users shall commit to understanding their role and responsibility in helping to ensure the security of DMV data and systems.	
2.7	Effective Date of DMV Information Security Policy	
2.7	This Information Security Policy will be effective immediately on approval by the Commissioner.	
2.8	Policy Content, Organization and Use	
2.8	**Content** Most content in this Policy is based on VITA's SEC501-07 *Information Security Standard* (draft), which is in turn based on National Institute of Standards and Technology (NIST) SP800-53 rev. 3*Security and Privacy Controls for Federal Information Systems and Organizations* . The Agency must also comply with Payment Card Industry (PCI) *Data Security Standard (DSS) v2.0* , due to citizens' use of credit and debit cards when transacting business with DMV. Finally, there are DMV-specific sections that address the unique needs of the Agency, and were generally carried over from DMV IT SECURITY POLICY Version 1.7 after being revised as needed. **Organization** This Policy combines elements of an information security policy, with accompanying information security standards, to address all requriements for the Agency in a single document. The main document is comprised of policy statements, such as Access Control and Configuration Management; these statements list the individual controls that are used to implement that policy, and the DMV-VITA Appendix documents those controls in detail. Every section in the Policy and the DMV-VITA Appendix is cross-referenced against PCI security requirements; PCI requirements with no corresponding VITA requirement are documented in the PCI Appendix. There is also a cross-reference of PCI vs VITA security requirements in the PCI-VITA_Cross-Reference Appendix. **Use** For general understanding, the policy statements provide an overview of the policy's intent in "Supplemental Guidance" sections. The security controls it includes are listed in the "Controls" section, and any exceptions to the Policy-wide Scope statement in Section 2.2 are also noted. The high-level PCI requirements addressed by the policy are listed under "PCI Compliance". For detailed understanding, refer to the specific controls in the DMV-VITA Appendix. Each section documents the control and specific details of its implementation, including a "Supplemental Guidance" section to help explain the control and provide examples in many cases. If there are any additional security requirements for sensitive systems, they are included in the section "Control Enhancements for Sensitive Systems". Lastly, the specific PCI requirements addressed by the control are listed under "PCI Compliance". In cases where Agency-specific requirements are specified, they are included in section "DMV-Specific Requirements". **NOTE:** Controls including "COV" in the name (for instance AC-2-COV ACCOUNT MANAGEMENT (COV)) were added by VITA's Commonwealth Security. These controls are in addition to those specified by the NIST security standard, and shall be requirements for all Commonwealth agencies and systems.	

3.0	**DMV-Specific Security Program Requirements**	
3.1	DMV IT Security Roles	
3.1.1	Agency Head	
3.1.1	The DMV Commissioner is responsible for the security of the Agency's information and IT systems. The Commissioner's information security responsibilities include the following: a. Designate an Information Security Officer (ISO) for the agency and provide the person's name, title (IT Security Director) and contact information to VITA no less than biennially. b. Maintain an information security program that is sufficient to protect the Agency's information and IT systems, and that is documented and effectively communicated. c. Review and approve DMV's Business Impact Analyses (BIA), Risk Assessments (RA), and Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable. d. Comply with the current version of the IT Security Audit Standard (COV ITRM Standard SEC502). The IT Security Audit activities must include, but are not limited to: • Require an Agency plan for IT security audits be developed and implemented, and submit this plan to the Chief Information Security Officer (CISO) for the Commonwealth; • Ensure planned audits are conducted; • Receive reports of audit results; • Require that Corrective Action Plans are developed and executed to address audit findings; and • Report to the CISO all IT security audit findings and progress in implementing required corrective actions, if any. e. Facilitate the communication process between IT staff and those in other areas of the agency. f. Establish a program of information security safeguards. g. Provide the resources required for employees to appropriately secure DMV information and systems. h. Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require explicit approval by authorized parties. (PCI 12.3, 12.3.1) i. Assign to an individual or team information security management responsibilities. (PCI 12.5)	
3.1.2	Deputy Commissioner/Chief Information Officer (CIO)	
3.1.2	The Deputy Commissioner/CIO is responsible for the management of Information Technology Services (ITS) at DMV. The Deputy Commissioner/CIO is the direct supervisor of the IT Security Director/ISO.	

3.1.3	Information Security Officer (ISO) (DMV IT Security Director)	
3.1.3	DMV's ISO has the title of IT Security Director. The IT Security Director is responsible for developing and managing the DMV's information security program. Working under the direction of the Deputy Commissioner/CIO, the IT Security Director's duties include: a. Develop and manage an Agency information security program that meets or exceeds the requirements of COV information security policies and standards in a manner commensurate with risk. b. Verify and validate that all DMV IT systems and data are classified for sensitivity. c. Develop and maintain an information security awareness and training program for all staff, including employees, contractors, consultants and IT service providers. d. Maintain liaison with the CISO, coordinating efforts and providing Agency-specific security information as required. e. Implement and maintain the appropriate balance of protective, detective and corrective controls for DMV IT systems commensurate with data sensitivity, risk and systems criticality. f. 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.	
3.1.3	g. Designates the ISO responsibilities and conditions under which they are delegated to the Deputy IT Security Director, who serves as backup ISO. h. Develop usage policies for critical technologies and define proper use of these technologies. Ensure these usage policies require explicit approval by authorized parties. (PCI 12.3, 12.3.1) i. Establish, document, and distribute security policies and procedures. (PCI 12.5.1) j. Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations. (PCI 12.5.3) k. Provide all policy changes to management for review and approval within thirty (30) days of their development. l. Review and assess annually the Information Security policy for new or changed requirements, either internal or external, including changes in the COV or DMV IT environment. This will occur in September of each year. m. ISO and designated IT Security staff will actively participate in Commonwealth IT security groups, including the Information Security Officers Advisory Group, to be aware of Commonwealth security changes.	
3.1.4	System Owner	
3.1.4	The System Owner is the DMV manager responsible for operating and maintaining a DMV IT system. The System Owner's information security responsibilities include the following: a. Require that all IT system users complete security awareness training prior to receiving access to the system, or as soon as possible after, and at least annually thereafter. b. Manage system risk and develop any additional information security policies and procedures required to protect the system in a manner commensurate with risk. c. Maintain compliance with COV information security policies and standards in all IT system activities. d. Maintain compliance with requirements specified by Data Owners for the handling of data processed by the system. e. Designate a System Administrator for the system. Note: Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner, upon request, the CIO of the Commonwealth will determine the System Owner.	

3.1.5	Data Owner	
3.1.5	The Data Owner is the DMV manager responsible for the policy and practice decisions regarding data captured, processed, stored and/or transmitted by an IT system, and is responsible for the following: a. Evaluate and classify sensitivity of the data. b. Define protection requirements for the data based on the sensitivity of the data, any legal or regulatory requirements, and business needs. c. Communicate data protection requirements to the System Owner. d. Define requirements for access to the data.	
3.1.6	System Administrator	
3.1.6	The System Administrator is a technical resource who implements, operates and supports system(s) at the direction of the System Owner, Data Owner, and/or Data Custodian. The System Administrator handles day-to-day administration of DMV IT system(s), and implements security controls and other requirements of the agency information security program on systems for which they are responsible.	
3.1.7	Data Custodian	
3.1.7	Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following: a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage. b. Manage and maintain data as directed by its Data Owner and in compliance with COV information security policies and standards. c. Provide Data Owners with access, usage and other reports regarding the data they are guardians of.	
3.1.8	IT System Users	
3.1.8	All users of DMV IT systems including employees, contractors, consultants and vendors are responsible for the following: a. Read and comply with DMV Information Security Policy requirements. b. Report actual or suspected information security incidents to the IT Security Director and their DMV manager. c. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.	
3.2	General Facilities Safety and Security	
3.2.1	DMV's practices and guidelines for physical security in general can be found at the following link on myDMV (internal site): Maintaining Safety and Security at DMV - http://mydmv/intranet/securityindex.shtml	

4.0	**COV Information Security Activities**	
4.1	Business Impact Analysis	
4.1.1	Purpose Business Impact Analysis (BIA) delineates the steps necessary for DMV to identify its business functions, identify those agency business functions that are essential to an agency's mission, and identify the resources that are required to support these essential agency business functions. Note: The requirements below address only the IT aspects of BIA and do not require that DMV to develop a BIA separate from that which they develop to meet the BIA requirements specified by the Virginia Department of Emergency Management (VDEM). DMV shall create a single BIA, which meets both the requirements of this Standard, and those specified by VDEM, and should consult the VDEM Continuity of Operation Planning Manual for non-IT related BIA requirements. Requirements 1. The Commissioner shall require the participation of System Owners and Data Owners in the development of the agency's BIA. 2. The Commissioner shall identify DMV business functions. 3. The Commissioner shall identify essential business functions. Note: A business function is essential if disruption or degradation of the function prevents the agency from performing its mission, as described in the agency mission statement. 4. The Commissioner shall identify dependent functions. Determine and document any additional functions on which each essential business function depends. These dependent functions are essential functions as well. . 5. The Commissioner shall, 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. 6. The IT Security Director shall use the IT information documented in the BIA report as a primary input to IT System and Data Sensitivity Classification, Risk Assessment, and IT Contingency Planning. 7. The IT Security Director shall conduct periodic review and revision of the agency BIA, as needed, but at least once every three years	
4.2	IT Security Audits	
4.2.1	Purpose IT Security Audit requirements define the steps necessary to assess whether IT security controls implemented to mitigate risks are adequate and effective. Note: In accordance with the Code of Virginia § 2.2-2009, the requirements of this section apply only to "all executive branch and independent agencies and institutions of higher education." Requirements 1. For each IT system classified as sensitive, the IT Security Director shall 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). 2. The IT Security Director is responsible for managing IT Security Audits.	

5.0	**Payment Card Industry Data Security Standard (PCI-DSS) Requirements**	
5.1	Background	
5.1	The Payment Card Industry Data Security Standard (PCI DSS) Program is a mandated set of security standards that were created by the major credit card companies to offer merchants and service providers a complete, unified approach to safeguarding cardholder data for all credit card brands. In September of 2006, a group of five leading payment brands including American Express, Discover Financial Services, JCB, MasterCard Worldwide and Visa International jointly announced formation of the PCI Security Standards Council, an independent council established to manage ongoing evolution of the PCI standard. The PCI Data Security Standard requirements apply to all payment card network members, merchants and service providers that store, process or transmit cardholder data. The requirements apply to all methods of credit card processing, from manual to computerized; the most comprehensive and demanding of which apply to e-commerce websites, and retail POS systems that process credit cards over the Internet. This document addresses all the requirements of the Payment Card Industry Data Security Standard (PCI DSS). For more information about this standard visit the official website at: https://www.pcisecuritystandards.org.	
5.2	Approach	
5.2	Where feasible, PCI information security requirements are integrated with requirements specified by VITA or DMV. The policy statement for each control family outlines general cross-reference information between VITA and PCI security requirements, with specific controls-to-PCI requirements detailed for each VITA or DMV control. Additionally, a PCI to VITA control cross- reference is in Appendix PCI. PCI-specific sections document the controls that have no corresponding VITA/DMV control; these sections are clearly marked, and apply ONLY to systems or components that meet the criteria detailed in section 5.3, Scope.	
5.3	Scope	
5.3	The PCI requirements apply to all "system components." System components are defined as any network component, server, or application that is included in or connected to the cardholder data environment. The cardholder data environment is defined as part of the network that possesses cardholder data or sensitive authentication data. For example, the following types of systems would be in scope for compliance within any environment: - Systems storing cardholder data (e.g. databases, PC's used by accounting for generating reports) - Systems processing cardholder data (e.g. web servers, application servers, etc) - Network devices transporting or directing cardholder traffic (e.g. border router, DMZ firewall, intranet firewall, etc) - Devices that create media containing cardholder data (e.g. fax machine, printer, backup tape silo) - Support systems (e.g. Active Directory, syslog server, IDS, PC's performing support functions such as system administration, etc) PCI data security requirements apply to all personnel, including employees, contractors, consultants, vendors and any other personnel who have access to cardholder or transaction data, or the systems on which that data is processed, stored or transmitted. Compliance exception requests must be made following the procedure in section 1.4 of this document.	

General Guidance on NIST-based Control Families and Security Controls:

Each Control Family includes a policy and procedure(s) to effectively implement the security controls that comprise the family. Control Families group individual security controls into logical, coherent approaches to protect DMV data and systems; some examples of control families are Access Control, Awareness and Training and Incident Response.
These policies and procedures comply with applicable laws, regulations, policies, standards, and guidance. Their implementation on individual systems may vary, depending on a risk-based assessment of security requirements, the sensitivity of the specific system, as well as the data it houses. DMV's risk management strategy is a key factor in developing these security policies and procedures.

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
2.1	***FAMILY:*** *ACCESS CONTROL*	***CLASS:*** *TECHNICAL*
AC-1	**ACCESS CONTROL POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates annually:	
a.	A formal, documented access control policy; and	
b.	Formal, documented procedures to implement the access control policy and associated access controls.	
	Controls: AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-4 INFORMATION FLOW ENFORCEMENT AC-5 SEPARATION OF DUTIES AC-6 LEAST PRIVILEGE AC-7 UNSUCCESSFUL LOGIN ATTEMPTS AC-8 SYSTEM USE NOTIFICATION AC-8-COV SYSTEM USE NOTIFICATION (COV) AC-10 CONCURRENT SESSION CONTROL AC-11 SESSION LOCK AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION AC-17 REMOTE ACCESS AC-17-COV REMOTE ACCESS (COV) AC-18 WIRELESS ACCESS AC-18-COV WIRELESS ACCESS (COV) AC-19 ACCESS CONTROL FOR MOBILE DEVICES AC-20 USE OF EXTERNAL INFORMATION SYSTEMS AC-20-COV USE OF EXTERNAL INFORMATION SYSTEMS (COV) AC-21 USER-BASED COLLABORATION AND INFORMATION SHARING AC-22 PUBLICLY ACCESSIBLE CONTENT	
	Purpose: This Policy implements the DMV Access Control Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Access Control Policy specifies the technical controls required to properly regulate access and use of DMV information and systems. It includes controls and procedures to: - provision accounts including creation, change and deletion - grant proper levels of access and authorization based on job functions and responsibilities - enforce those levels consistently - define safe access to DMV & external systems by a variety of technologies Two concepts are key to properly applying these controls: Least Privilege, granting the minimum level of access to information and systems needed to perform one's job; and Separation of Duties, dividing job functions so proper checks and oversight are in place to minimize the risk of abuse or fraud.	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	PCI Compliance: The Access Control Policy specifies technical controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 1: Install and maintain a firewall configuration to protect cardholder data - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters - Requirement 4: Encrypt transmission of cardholder data across open, public networks - Requirement 5: Use and regularly update anti-virus software or programs - Requirement 6: Develop and maintain secure systems and applications - Requirement 7: Restrict access to cardholder data by business need to know - Requirement 8: Assign a unique ID to each person with computer access - Requirement 11: Regularly test security systems and processes - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Access Control family are cross-referenced to specific PCI DSS requirements.	
2.2 **AT-1**	***FAMILY:*** *AWARENESS AND TRAINING* **SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES**	***CLASS:*** *OPERATIONAL* Previous SEC 501-06 Control References: 2.2.4.7/2.2.5.3/8.3.2.1-7
	The organization develops, disseminates, and reviews/updates annually or more often as necessary:	
a.	A formal, documented security awareness and training policy; and	
b.	Formal, documented procedures to implement the security awareness and training policy and associated security awareness and training controls	
	Controls: AT-2 SECURITY AWARENESS AT-2-COV SECURITY AWARENESS (COV) AT-3 SECURITY TRAINING AT-4 SECURITY TRAINING RECORDS AT-5 CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS	
	Purpose: This Policy implements the DMV Security Awareness and Training Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Scope: This policy applies to all personnel and locations of DMV; however, the ISO can grant exceptions based on special circumstances, which shall be considered on a case-by-case basis.	
	Supplemental Guidance: The Security Awareness and Training Policy specifies the operational controls required to adequately instruct users of their responsibilities when using DMV information and systems. It includes controls and procedures to: - document the purpose, scope, frequency and timing of Security Awareness training - outline required content - define types of training - ensure compliance by proper record-keeping The key concept to continually reinforce is that DMV's overall security posture is only as strong as its weakest link; uninformed or poor decisions made by its people can undo the most sophisticated technical controls. The legal, financial and reputational penalties for breaches in security are very real and very costly to the individual(s) accountable for the breach as well as the Agency as a whole.	
	PCI Compliance: The Security Awareness and Training Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 8: Assign a unique ID to each person with computer access - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Security Awareness and Training family are cross-referenced to specific PCI DSS requirements.	
2.3 **AU-1**	***FAMILY:*** *AUDIT AND ACCOUNTABILITY* **AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES**	***CLASS:*** *TECHNICAL* Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented audit and accountability policy; and	
b.	Formal, documented procedures to implement the audit and accountability policy and associated audit and accountability controls	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Controls: AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS AU-4 AUDIT STORAGE CAPACITY AU-5 RESPONSE TO AUDIT PROCESSING FAILURES AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING AU-8 TIME STAMPS AU-9 PROTECTION OF AUDIT INFORMATION AU-11 AUDIT RECORD RETENTION AU-12 AUDIT GENERATION	
	Purpose: This Policy implements the DMV Audit and Accountability Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Audit and Accountability Policy specifies the technical controls required to provide auditing capability for DMV IT systems. It includes controls and procedures to: - define which system events to capture and at what level of detail - ensure the system's logging capacity meets requirements for volume and retention - specify required protections for logging mechanisms and log content Careful analysis is required to strike the right balance between under- and over-logging of system events. Large systems can generate overwhelming volumes of audit/log records that make any use of the captured data nearly impossible. A second key is to ensure the logging function is highly reliable and protected, to minimize risks of failure, manipulation or corruption. Meeting these two requirements will help to ensure effective and accurate auditing capability.	
	PCI Compliance: The Audit and Accountability Policy specifies technical controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 10: Track and monitor all access to network resources and cardholder data Individual controls in the Audit and Accountability family are cross-referenced to specific PCI DSS requirements.	
2.4	***FAMILY** : SECURITY ASSESSMENT AND AUTHORIZATION*	***CLASS:** MANAGEMENT*
CA-1	**SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	Formal, documented security assessment and authorization policies; and	
b.	Formal, documented procedures to facilitate the implementation of the security assessment and authorization policies and associated security assessment and authorization controls	
	Controls: CA-2 SECURITY ASSESSMENTS CA-3 INFORMATION SYSTEM CONNECTIONS CA-3-COV INFORMATION SYSTEM CONNECTIONS (COV) CA-6 SECURITY AUTHORIZATION CA-7 CONTINUOUS MONITORING	
	Purpose: This Policy implements the DMV Security Assessment and Authorization Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Security Assessment and Authorization Policy specifies the management controls required to assess and authorize the security of DMV IT systems. It includes controls and procedures to: - require Interconnection Security Agreements to explicitly document connections between DMV & external systems and define the data interfaces - designate the DMV executive authorizing the operation of Agency system(s) based on identified risks, mitigating controls and plans to remediate deficiencies - require a Continuous Monitoring program that includes managing system configurations and changes, assesses security controls and periodically reports on the security state of the system This Policy documents explicitly the external connections, the Agency executive accountable for security, and the process to proactively monitor the security status of DMV systems.	
	PCI Compliance: The Security Assessment and Authorization Policy specifies management controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Security Assessment and Authorization family are cross-referenced to specific PCI DSS requirements.	
2.5	***FAMILY:** CONFIGURATION MANAGEMENT*	***CLASS:** OPERATIONAL*

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
CM-1	**CONFIGURATION MANAGEMENT POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: 10.4
	The organization develops, disseminates, and reviews/updates at least once a year or after any demonstrated deficiency in the configuration management procedure	
a.	A formal, documented configuration management policy; and	
b.	Formal, documented procedures to implement the configuration management policy and associated configuration management controls	
	Controls: CM-2 BASELINE CONFIGURATION CM-2-COV BASELINE CONFIGURATION (COV) CM-3 CONFIGURATION CHANGE CONTROL CM-3-COV CONFIGURATION CHANGE CONTROL (COV) CM-4 SECURITY IMPACT ANALYSIS CM-5 ACCESS RESTRICTIONS FOR CHANGE CM-6 CONFIGURATION SETTINGS CM-7 LEAST FUNCTIONALITY CM-8 INFORMATION SYSTEM COMPONENT INVENTORY CM-9 CONFIGURATION MANAGEMENT PLAN	
	Purpose: This Policy implements the DMV Configuration Management Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Configuration Management Policy specifies the operational controls required to manage changes to DMV system configurations and applications. It includes controls and procedures to: - develop a configuration management plan that addresses the who, what and how of securely implementing required changes to DMV IT systems - establish baseline system configurations based on secure, hardened benchmarks that enable only business-required services and functions - institute a Change Control Board that oversees and regulates a formal change management process that includes identifying authorized requestors, approvers and change implementers - require that changes be tested and assessed for potential impacts on security The implementation of changes to system configurations and applications is frequently the most risky of all IT activities. Unscheduled downtime, impaired functionality, degraded performance and invalidated security controls all are relatively common outcomes from change activities. Implementing a documented, controlled process for change, then enforcing it strictly, is essential to maintaining the stability and security of DMV systems.	
	PCI Compliance: The Configuration Management Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 1: Install and maintain a firewall configuration to protect cardholder data - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters - Requirement 6: Develop and maintain secure systems and applications - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Configuration Management family are cross-referenced to specific PCI DSS requirements.	
2.6	***FAMILY:*** *CONTINGENCY PLANNING*	***CLASS:*** *OPERATIONAL*
CP-1	**CONTINGENCY PLANNING POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: 3.1
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented contingency planning policy; and	
b.	Formal, documented procedures to implement the contingency planning policy and associated contingency planning controls	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Controls: CP-2 CONTINGENCY PLAN CP-3 CONTINGENCY TRAINING CP-4 CONTINGENCY PLAN TESTING AND EXERCISES CP-6 ALTERNATE STORAGE SITE CP-7 ALTERNATE PROCESSING SITE CP-8 TELECOMMUNICATIONS SERVICES CP-9 INFORMATION SYSTEM BACKUP CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION	
	Purpose: This Policy implements the DMV Contingency Planning Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Contingency Planning Policy specifies the operational controls required to continue or recover the operation of DMV IT systems due to threatened or actual hazards the Agency may face. It includes controls and procedures to: - develop a contingency plan that details the who, what, when, where and how of recovering DMV systems that support essential business functions - require a training and exercise program to ensure personnel understand and can execute the plan based on their contingency roles - identify alternate resources, including secondary storage, processing and telecommunications, in the event primary resources are destroyed or disabled - ensure reliable data backups occur with appropriate protection of media and proven recoverability, based on business requirements These controls are crucial to sustaining the Agency mission in the face of natural or man-made hazards. They relate to other planning efforts including Emergency Response and Continuity of Operations Plans that DMV has developed. To maximize effectiveness and efficiency, these plans should coordinate their activities and resources.	
	PCI Compliance: The Contingency Planning Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 9: Restrict physical access to cardholder data - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Contingency Planning family are cross-referenced to specific PCI DSS requirements.	
2.7	***FAMILY:*** *IDENTIFICATION AND AUTHENTICATION*	***CLASS:*** *TECHNICAL*
IA-1	**IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented identification and authentication policy; and	
b.	Formal, documented procedures to implement the identification and authentication policy and associated identification and authentication controls	
	Controls: IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IA-4 IDENTIFIER MANAGEMENT IA-5 AUTHENTICATOR MANAGEMENT IA-6 AUTHENTICATOR FEEDBACK IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION IA-8 IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)	
	Purpose: This Policy implements the DMV Identification and Authentication Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Identification and Authentication Policy specifies the technical controls required to uniquely identify and authenticate users and devices on DMV IT systems. It includes controls and procedures to: - ensure unique identifiers exist for each user and device, to validate their identity as well as enable individual accountability for system activities - related to control AC-2 (Account Management), implement a process to manage the request, approval, setup and removal of user accounts (or identifiers) - if the DMV system uses encryption, ensure it authenticates securely to cryptographic module(s) that encrypt/decrypt data These technical controls tie closely to the Access Control (AC) family; however "identifiers" as used in this policy refers to identifying devices as well as users. Uniquely identifying users and devices is crucial to implementing and enforcing most technical security controls; although a distinction is made in controls IA-2 and IA-8 between "Organizational Users" (internal users) and "Non-Organizational Users" (external users), there is no difference in the need to accurately identify and authenticate them.	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	PCI Compliance: The Identification and Authentication Policy specifies technical controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters - Requirement 6: Develop and maintain secure systems and applications - Requirement 8: Assign a unique ID to each person with computer access - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Identification and Authentication family are cross-referenced to specific PCI DSS requirements.	
2.8	***FAMILY:*** *INCIDENT RESPONSE*	***CLASS:*** *OPERATIONAL*
IR-1	**INCIDENT RESPONSE POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: 9.4.2
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented incident response policy; and	
b.	Formal, documented procedures to implement the incident response policy and associated incident response controls.	
	Controls: IR-1-COV INCIDENT RESPONSE (COV) IR-2 INCIDENT RESPONSE TRAINING IR-3 INCIDENT RESPONSE TESTING AND EXERCISES IR-4 INCIDENT HANDLING IR-4-COV INCIDENT HANDLING (COV) IR-4-COV-2 INCIDENT HANDLING (COV-2) IR-5 INCIDENT MONITORING IR-5-COV INCIDENT MONITORING (COV) IR-6 INCIDENT REPORTING IR-6-COV INCIDENT REPORTING (COV) IR-7 INCIDENT RESPONSE ASSISTANCE IR-8 INCIDENT RESPONSE PLAN	
	Purpose: This Policy implements the DMV Incident Response Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Incident Response Policy specifies the operational controls required to manage IT security incident response on DMV systems. It includes controls and procedures to: - develop an incident response plan that details the who, what, when, where and how of handling, monitoring and reporting IT security incidents - require a training and exercise program to ensure personnel understand and can execute the plan based on their incident response roles - include procedures to detect, analyze, contain, eradicate and recover from incidents Currently, it is obvious that IT security incidents are inevitable; those guarding DMV IT systems must be 100% successful to prevent all attacks, and those with ill intent must only succeed once. It is not rational to assume this will occur, so planning for events that negatively affect Agency systems must be done. Incident Response encompasses a wide range of activities and involves all DMV personnel - from system users who must report events they see or experience, to senior management who must commit resources and focus to rapidly address and resolve incidents or potential incidents. A strong response can minimize the damage done to data and systems, and help ensure that DMV continues serving Commonwealth citizens.	
	PCI Compliance: The Incident Response Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 11: Regularly test security systems and processes - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Incident Response family are cross-referenced to specific PCI DSS requirements.	
2.9	***FAMILY:*** *MAINTENANCE*	***CLASS:*** *OPERATIONAL*
MA-1	**SYSTEM MAINTENANCE POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented information system maintenance policy; and	
b.	Formal, documented procedures to implement the information system maintenance policy and associated system maintenance controls	
	Controls: MA-2 CONTROLLED MAINTENANCE MA-5 MAINTENANCE PERSONNEL	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Purpose: This Policy implements the DMV System Maintenance Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The System Maintenance Policy specifies the operational controls required to securely maintain and repair DMV IT systems. It includes controls and procedures to: - ensure a maintenance program is established to properly maintain and repair IT systems and components; it includes scheduling, performing maintenance/repair activities and adequately documenting their execution - who, what, when, and device or component - ensure security controls are not altered or negatively impacted by maintenance or repair - protect appropriately equipment that requires offsite maintenance, e.g., sanitize storage devices before moving them offsite - require that maintenance organizations and their personnel be properly authorized prior to gaining physical or remote access to DMV systems The System Maintenance Policy ensures that physical and logical access controls extend to vendors, contractors and others who provide maintenance or repair, and that those activities are actively managed by the Agency.	
	PCI Compliance: The System Maintenance Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the System Maintenance family are cross-referenced to specific PCI DSS requirements.	
2.10 **MP-1**	***FAMILY:*** *MEDIA PROTECTION* **MEDIA PROTECTION POLICY AND PROCEDURES**	***CLASS:*** *OPERATIONAL* Previous SEC 501-06 Control References: 3.4
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented media protection policy; and	
b.	Formal, documented procedures to implement the media protection policy and associated media protection controls.	
	Controls: MP-2 MEDIA ACCESS MP-3 MEDIA MARKING MP-4 MEDIA STORAGE MP-5 MEDIA TRANSPORT MP-6 MEDIA SANITIZATION MP-6-COV MEDIA SANITIZATION (COV)	
	Purpose: This Policy implements the DMV Media Protection Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Media Protection Policy specifies the operational controls required to securely handle, transport, store and dispose of media that contains DMV information. It includes controls and procedures to: - ensure only authorized personnel have physical access to any media that Agency information resides on - protect appropriately any media in storage or transit - require secure sanitizing of media prior to disposal or reuse This Policy implements controls to secure media, both digital and non-digital, that stores DMV information. The level of control should correspond to the sensitivity of the data being protected, and the level of protection should remain consistent from creation through destruction. The Policy includes security controls for media storage, transit and disposal.	
	PCI Compliance: The Media Protection Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 9: Restrict physical access to cardholder data Individual controls in the Media Protection family are cross-referenced to specific PCI DSS requirements.	
2.11 **PE-1**	***FAMILY****: PHYSICAL AND ENVIRONMENTAL PROTECTION* **PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES**	***CLASS:*** *OPERATIONAL* Previous SEC 501-06 Control References: 7.2
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented physical and environmental protection policy; and	
b.	Formal, documented procedures to implement the physical and environmental protection policy and associated physical and environmental protection controls	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Controls: PE-1-COV PHYSICAL AND ENVIRONMENTAL PROTECTION (COV) PE-2 PHYSICAL ACCESS AUTHORIZATIONS PE-3 PHYSICAL ACCESS CONTROL PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM PE-5 ACCESS CONTROL FOR OUTPUT DEVICES PE-6 MONITORING PHYSICAL ACCESS PE-7 VISITOR CONTROL PE-8 ACCESS RECORDS (VISITOR) PE-9 POWER EQUIPMENT AND POWER CABLING PE-10 EMERGENCY SHUTOFF PE-11 EMERGENCY POWER PE-13 FIRE PROTECTION PE-14 TEMPERATURE AND HUMIDITY CONTROLS PE-15 WATER DAMAGE PROTECTION PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS	
	Purpose: This Policy implements the DMV Physical and Environmental Protection Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Physical and Environmental Protection Policy specifies the operational controls required to secure and protect DMV offices, and especially the restricted access areas that house IT and system components. It includes controls and procedures to: - require positive identification for access to DMV facilities except public areas, and explicit and separate authorization to enter IT or network equipment areas - control and monitor physical access by all personnel, specifically distinguishing visitors from employees and other facility residents - protect equipment from functional outages and/or damage from various causes (e.g., fire, temperature/humidity, power failure) Physical and Environmental Protection controls regulate and manage access of personnel, specifically to areas housing IT/network equipment. They physically implement the Least Privilege concept; only those with a current business need should have access to these secure areas. These controls also specify steps to protect systems and equipment from a variety of environmental hazards.	
	PCI Compliance: The Physical and Environmental Protection Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 9: Restrict physical access to cardholder data - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Physical and Environmental Protection family are cross-referenced to specific PCI DSS requirements.	
2.12 **PL-1**	***FAMILY:*** *PLANNING* **SECURITY PLANNING POLICY AND PROCEDURES**	***CLASS:*** *MANAGEMENT* Previous SEC 501-06 Control References: 1.4
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented security planning policy; and	
b.	Formal, documented procedures to implement the security planning policy and associated security planning controls	
	Controls: PL-2 SYSTEM SECURITY PLAN PL-2-COV SYSTEM SECURITY PLAN (COV) PL-4 RULES OF BEHAVIOR PL-4-COV RULES OF BEHAVIOR (COV) PL-6 SECURITY-RELATED ACTIVITY PLANNING	
	Purpose: This Policy implements the DMV Security Planning Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Supplemental Guidance: The Security Planning Policy specifies the management controls required to plan and coordinate IT system security activities; it also describes proper use of DMV systems. It includes controls and procedures to: - require that a System Security Plan be developed, based on the Risk Assessment, that details each system's security posture including actual and planned controls - define and regulate acceptable use of DMV systems (i.e., Rules of Behavior) - specify that security-related activities like assessments, audits, exercises, etc. be planned and coordinated to maximize efficiency and minimize impact on the Agency Security Planning implements controls to require a regimented approach to system security, as well as details the acceptable use of DMV IT systems and resources.	
	PCI Compliance: The Security Planning Policy specifies management controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 8: Assign a unique ID to each person with computer access - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Security Planning family are cross-referenced to specific PCI DSS requirements.	
2.13	***FAMILY:*** *PERSONNEL SECURITY*	***CLASS:*** *OPERATIONAL*
PS-1	**PERSONNEL SECURITY POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented personnel security policy; and	
b.	Formal, documented procedures to implement the personnel security policy and associated personnel security controls.	
	Controls: PS-2 POSITION CATEGORIZATION PS-3 PERSONNEL SCREENING PS-4 PERSONNEL TERMINATION PS-5 PERSONNEL TRANSFER PS-6 ACCESS AGREEMENTS PS-7 THIRD-PARTY PERSONNEL SECURITY PS-8 PERSONNEL SANCTIONS	
	Purpose: This Policy implements the DMV Personnel Security Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Personnel Security Policy specifies the operational controls that regulate personnel access to DMV systems. It includes controls and procedures to: - require that screening or background check occurs before granting personnel access to Agency systems - manage access to ensure that terminations, transfers and disciplinary actions trigger a prompt change in system access, as required - require individuals to acknowledge through signed agreements their understanding and compliance with published policies, standards and guidelines - define security requirements for third-party personnel and their organizations These controls implement the operational aspects of regulating access to DMV systems and seek to manage the human risk that DMV IT systems and information are exposed to.	
	PCI Compliance: The Personnel Security Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 8: Assign a unique ID to each person with computer access - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Personnel Security family are cross-referenced to specific PCI DSS requirements.	
2.14	***FAMILY:*** *RISK ASSESSMENT*	***CLASS:*** *MANAGEMENT*
RA-1	**RISK ASSESSMENT POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: 2.6
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented risk assessment policy; and	
b.	Formal, documented procedures to implement the risk assessment policy and associated risk assessment controls.	
	Controls: RA-2 SECURITY CATEGORIZATION RA-3 RISK ASSESSMENT RA-5 VULNERABILITY SCANNING RA-5-COV VULNERABILITY SCANNING (COV)	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	Purpose: This Policy implements the DMV Risk Assessment Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The Risk Assessment Policy specifies the management controls that identify and assess risks to DMV systems, based on threats, vulnerabilities and mitigating controls. It includes controls and procedures to: - require the security categorization of each DMV system, based on sensitivity of data it processes, stores or transmits - direct that a Risk Assessment is performed to consider threats, vulnerabilities and the effect security controls have on reducing risk - ensure periodic vulnerability scanning is performed to identify system vulnerabilities and require their prompt remediation The Risk Assessment Policy is a cornerstone of DMV's Information Security Program. A risk-based approach to implementing security controls means the greatest risks, based on likelihood and impact, receive the greatest attention; effective security requires identifying and understanding risks the Agency faces.	
	PCI Compliance: The Risk Assessment Policy specifies management controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 6: Develop and maintain secure systems and applications - Requirement 11: Regularly test security systems and processes - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the Risk Assessment family are cross-referenced to specific PCI DSS requirements.	
2.15	***FAMILY:*** *SYSTEM AND SERVICES ACQUISITION*	***CLASS:*** *MANAGEMENT*
SA-1	**SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented system and services acquisition policy that includes information security considerations; and	
b.	Formal, documented procedures to implement the system and services acquisition policy and associated system and services acquisition controls.	
	Controls: SA-2 ALLOCATION OF RESOURCES SA-3 LIFE CYCLE SUPPORT SA-3-COV-1 LIFE CYCLE SUPPORT (COV-1) SA-3-COV-2 LIFE CYCLE SUPPORT (COV-2) SA-4 ACQUISITIONS SA-5 INFORMATION SYSTEM DOCUMENTATION SA-6 SOFTWARE USAGE RESTRICTIONS SA-6-COV SOFTWARE USAGE RESTRICTIONS (COV) SA-7 USER-INSTALLED SOFTWARE SA-8 SECURITY ENGINEERING PRINCIPLES SA-9 EXTERNAL INFORMATION SYSTEM SERVICES SA-10 DEVELOPER CONFIGURATION MANAGEMENT SA-11 DEVELOPER SECURITY TESTING	
	Purpose: This Policy implements the DMV System and Services Acquisition Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The System and Services Acquisition Policy specifies the management controls required to develop or procure secure IT systems and services. It includes controls and procedures to: - require budget and resource allocations specifically to meet information security requirements - ensure security is designed into projects and applications during planning efforts, and carried through to project or application shutdown - specify general engineering, design, coding and testing practices for developing secure applications - require use of only Agency approved software, that complies with all applicable contract and copyright laws - define the security requirements vendors must meet when the Agency procures external Information System Services, and detail DMV's oversight and compliance monitoring responsibility This Policy establishes controls to develop or procure systems or services that meet DMV security requirements. It focuses on building security into the deliverables obtained by either process to ensure that effective security controls are integral parts of the application. It also requires that software meets legal and DMV requirements before installation and use.	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
	PCI Compliance: The System and Services Acquisition Policy specifies management controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 3: Protect stored cardholder data - Requirement 6: Develop and maintain secure systems and applications - Requirement 7: Restrict access to cardholder data by business need to know - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the System and Services Acquisition family are cross-referenced to specific PCI DSS requirements.	
2.16	***FAMILY:*** *SYSTEM AND COMMUNICATIONS PROTECTION*	***CLASS:*** *TECHNICAL*
SC-1	**SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented system and communications protection policy; and	
b.	Formal, documented procedures to implement the system and communications protection policy and associated system and communications protection controls	
	Controls: SC-2 APPLICATION PARTITIONING SC-3 SECURITY FUNCTION ISOLATION SC-4 INFORMATION IN SHARED RESOURCES SC-5 DENIAL OF SERVICE PROTECTION SC-7 BOUNDARY PROTECTION SC-8 TRANSMISSION INTEGRITY SC-8-COV TRANSMISSION INTEGRITY (COV) SC-9 TRANSMISSION CONFIDENTIALITY SC-9-COV TRANSMISSION CONFIDENTIALITY (COV) SC-10 NETWORK DISCONNECT SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT SC-13 USE OF CRYPTOGRAPHY SC-14 PUBLIC ACCESS PROTECTIONS SC-17 PUBLIC KEY INFRASTRUCTURE CERTIFICATES SC-20 SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE) SC-23 SESSION AUTHENTICITY SC-28 PROTECTION OF INFORMATION AT REST	
	Purpose: This Policy implements the DMV System and Communications Protection Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The System and Communications Protection Policy specifies the technical controls required to protect DMV IT systems and network communications. It includes controls and procedures to: - require functional separation of applications and security - specify various network protections, including boundary and perimeter security - define generally encryption best practices - require protection of public information This Policy defines a wide variety of controls to secure DMV IT systems and networks. Most are established and managed by technical resources, with two exception; SC-8-COV and SC-9-COV. The network- and application-oriented controls in this family generally use techniques such as partitions, boundaries and segments to isolate disparate functions - user vs. administrative, security vs. non-security, internal vs. external - to maximize security. Most of the remaining controls address encryption for data at rest or in motion, or the administrative structure to manage encryption in the Agency.	
	PCI Compliance: The System and Communications Protection Policy specifies technical controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 1: Install and maintain a firewall configuration to protect cardholder data - Requirement 4: Encrypt transmission of cardholder data across open, public networks - Requirement 6: Develop and maintain secure systems and applications - Requirement 8: Assign a unique ID to each person with computer access Individual controls in the System and Communications Protection family are cross-referenced to specific PCI DSS requirements.	

No.	Control Family / Control Name / Guidance	Class / Reference / Comments
2.17	***FAMILY:*** *SYSTEM AND INFORMATION INTEGRITY*	***CLASS:*** *OPERATIONAL*
SI-1	**SYSTEM AND INFORMATION INTEGRITY POLICY AND PROCEDURES**	Previous SEC 501-06 Control References: None
	The organization develops, disseminates, and reviews/updates at least once a year:	
a.	A formal, documented system and information integrity policy; and	
b.	Formal, documented procedures to implement the system and information integrity policy and associated system and information integrity controls	
	Controls: SI-2 FLAW REMEDIATION SI-2-COV FLAW REMEDIATION (COV) SI-3 MALICIOUS CODE PROTECTION SI-3-COV MALICIOUS CODE PROTECTION (COV) SI-4 INFORMATION SYSTEM MONITORING SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES SI-7 SOFTWARE AND INFORMATION INTEGRITY SI-8 SPAM PROTECTION SI-9 INFORMATION INPUT RESTRICTIONS SI-10 INFORMATION INPUT VALIDATION SI-11 ERROR HANDLING	
	Purpose: This Policy implements the DMV System and Information Integrity Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance of the policy.	
	Supplemental Guidance: The System and Information Integrity Policy specifies the operational controls required to ensure integrity of DMV IT systems and data. It includes controls and procedures to: - require that information system flaws or bugs are promptly corrected - ensure malicious code protection, including spam, is deployed throughout the Agency on servers, workstations and mobile devices - specify internal and external monitoring requirements for DMV systems using a variety of tools and techniques - gather and distribute security alerts, advisories and directives from a variety of internal and external sources - restrict users' access to input data, and validate the data that is input This Policy defines a wide variety of controls to maintain the integrity of DMV IT systems and data. They are primarily implemented and managed by technical resources. The controls in this family are a combination of protective, detective and corrective controls that implement a multi-layered strategy to maintain system and data integrity.	
	PCI Compliance: The System and Information Integrity Policy specifies operational controls that address a variety of protections mandated by PCI DSS. The relevant high-level PCI requirements include: - Requirement 5: Use and regularly update anti-virus software or programs - Requirement 6: Develop and maintain secure systems and applications - Requirement 11: Regularly test security systems and processes - Requirement 12: Maintain a policy that addresses information security for all personnel Individual controls in the System and Information Integrity family are cross-referenced to specific PCI DSS requirements.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
2.1	***FAMILY:*** *ACCESS CONTROL*	***CLASS:*** *TECHNICAL*
AC-2	**ACCOUNT MANAGEMENT**	Previous SEC 501-06 Control References: 5.2.2
	Control: The organization manages information system accounts, including:	
a.	Identifying account types (i.e., individual, group, system, application, guest/anonymous, and temporary);	
b.	Establishing conditions for group membership;	
c.	Identifying authorized users of the information system and specifying access privileges;	
d.	Requiring appropriate approvals for requests to establish accounts;	
e.	Establishing, activating, modifying, disabling, and removing accounts;	
f.	Specifically authorizing and monitoring the use of guest/anonymous and temporary accounts;	
g.	Notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to-know/need-to-share changes;	
h.	Deactivating: (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users;	
i.	Granting access to the system based on: (i) a valid access authorization; (ii) intended system usage; and (iii) other attributes as required by the organization or associated missions/business functions; and	
j.	Reviewing accounts annually at a minimum.	
	Supplemental Guidance: Users requiring administrative privileges on information system accounts receive additional scrutiny by Information Security Officers responsible for approving such accounts and privileged access. Related controls: AC-3, AC-4, AC-5, AC-6, AC-10, AC-17, AC-19, AC-20, AU-9, IA-4, IA-5, CM-5, CM-6, MA-3, MA-4, MA-5, SA-7, SC-13, SI-9.	
	DMV-Specific Requirements: Remove/disable inactive user accounts at least every 90 days. PCI 8.5.5 VITA AC-2	
	Control Enhancements for Sensitive Systems:	
(2)	The information system automatically terminates temporary and emergency accounts after a predetermined period based on sensitivity and risk.	
(3)	The information system automatically disables inactive accounts if not used for a predefined period. **Note:** Agencies should strongly consider locking accounts that go unused for 90 consecutive days.	
(4)	The information system automatically audits account creation, modification, disabling, and termination actions and notifies, as required, appropriate individuals.	
(5)	The organization:	
(c)	Monitors for atypical usage of information system accounts; and	
(d)	Reports atypical usage to designated organizational officials.	
(7)	The organization:	
(b)	Tracks and monitors privileged role assignments.	
	Enhancement Supplemental Guidance: Privileged roles include, for example, key management, network and system administration, database administration, web administration.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel's job classification and function 7.1.3 Requirement for a documented approval by authorized parties specifying required privileges. 7.2.2 Assignment of privileges to individuals based on job classification and function. 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: 8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. 8.5.5 Remove/disable inactive user accounts at least every 90 days. 12.5.4 Administer user accounts, including additions, deletions, and modifications.	
AC-2-COV	**ACCOUNT MANAGEMENT (COV)**	Previous SEC 501-06 Control References: 5.2.2
1	**Control: If the IT system is classified as sensitive, prohibit the use of guest accounts.**	
2	Prohibit the use of shared accounts on all IT systems. Those systems residing on a guest network are exempt from this requirement.	
3	If the IT system is classified as sensitive, require requests for and approvals of emergency or temporary access 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.	
4	For all internal IT systems:	
a.	Require a documented request from the user to establish an account on any internal IT system.	
b.	Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.	
c.	Require confirmation of the account request and approval by the IT system user's supervisor and approval by the Data Owner or designee to establish accounts for all sensitive IT systems.	
d.	Require secure delivery of access credentials to the user based on information already on file.	
e.	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.	
f.	Promptly remove access when no longer required.	
5	For all external IT systems:	
a.	Require secure delivery of access credentials to users of all external IT systems.	
b.	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.	
c.	Require delivery of access credentials to users of all sensitive external IT systems by means of an alternate channel (i.e., U.S. Mail).	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
6	For all service and hardware accounts:	
a.	Document account management practices for all agency-created service accounts, including, but not limited to granting, administering and terminating accounts. If the service or hardware account is not used for interactive login with the system, the service or hardware account is exempt from the requirement to change the password at the interval defined in the Password Management section of this Standard	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel's job classification and function 7.1.3 Requirement for a documented approval by authorized parties specifying required privileges. 7.2.2 Assignment of privileges to individuals based on job classification and function. 12.5.4 Administer user accounts, including additions, deletions, and modifications.	
AC-3	**ACCESS ENFORCEMENT**	Previous SEC 501-06 Control References: 6.4.2
	Control: The information system enforces approved authorizations for logical access to the system in accordance with applicable policy.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	
(6)	The organization encrypts or stores sensitive data off-line in a secure location.	
	Enhancement Supplemental Guidance: The use of encryption by the organization reduces the probability of unauthorized disclosure of information and can also detect unauthorized changes to information. Removing information from online storage to offline storage eliminates the possibility of individuals gaining unauthorized access via a network. Related control: MP-4.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel's job classification and function 7.1.3 Requirement for a documented approval by authorized parties specifying required privileges. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. 7.2.2 Assignment of privileges to individuals based on job classification and function. And the Control aspect of: 12.5.5 Monitor and control all access to data.	
AC-4	**INFORMATION FLOW ENFORCEMENT**	Previous SEC 501-06 Control References: None
	Control: The information system enforces approved authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy.	
	Supplemental Guidance: Information flow control regulates where information is allowed to travel within an information system and between information systems (as opposed to who is allowed to access the information) and without explicit regard to subsequent accesses to that information. A few examples of flow control restrictions include: keeping export controlled information from being transmitted in the clear to the Internet, blocking outside traffic that claims to be from within the organization, and not passing any web requests to the Internet that are not from the internal web proxy. Information flow control policies and enforcement mechanisms are commonly employed by organizations to control the flow of information between designated sources and destinations (e.g., networks, individuals, devices) within information systems and between interconnected systems. Flow control is based on the characteristics of the information and/or the information path. Specific examples of flow control enforcement can be found in boundary protection devices (e.g., proxies, gateways, guards, encrypted tunnels, firewalls, and routers) that employ rule sets or establish configuration settings that restrict information system services, provide a packet-filtering capability based on header information, or message-filtering capability based on content (e.g., using key word searches or document characteristics). Mechanisms implemented by AC-4 are configured to enforce authorizations determined by other security controls. Related controls: AC-17, AC-19, AC-21, CM-7, SA-8, SC-2, SC-5, SC-7, SC-18.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. 1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ. 1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ. 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.) 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	
AC-5	**SEPARATION OF DUTIES**	Previous SEC 501-06 Control References: 8.2.2.8/2.2.4.10
	Control: The organization:	
a.	Separates duties of individuals as necessary, to prevent malevolent activity without collusion;	
b.	Documents separation of duties; and	
c.	Implements separation of duties through assigned information system access authorizations.	
	Supplemental Guidance: Examples of separation of duties include: (i) mission functions and distinct information system support functions are divided among different individuals/roles; (ii) different individuals perform information system support functions (e.g., system management, systems programming, configuration management, quality assurance and testing, network security); (iii) security personnel who administer access control functions do not administer audit functions; and (iv) different administrator accounts for different roles. Access authorizations defined in this control are implemented by control AC-3. Related controls: AC-3.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.4 Description of groups, roles, and responsibilities for logical management of network components. 6.4.2 Separation of duties between development/test and production environments.	
AC-6	**LEAST PRIVILEGE**	Previous SEC 501-06 Control References: 5.2.2.1/5.2.2.16
	Control: The organization employs the concept of least privilege, allowing only authorized accesses for users (and processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.	
	Supplemental Guidance: The access authorizations defined in this control are largely implemented by control AC-3. The organization employs the concept of least privilege for specific duties and information systems (including specific ports, protocols, and services) in accordance with risk assessments as necessary to adequately mitigate risk to organizational operations and assets, individuals, other organizations, and the Commonwealth. Related controls: AC-2, AC-3, CM-7.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization explicitly authorizes access to administrative accounts.	
	Enhancement Supplemental Guidance: Establishing system accounts, configuring access authorizations (i.e., permissions, privileges), setting events to be audited, and setting intrusion detection parameters are examples of security functions. Explicitly authorized personnel include, for example, security administrators, system and network administrators, system security officers, system maintenance personnel, system programmers, and other privileged users. Related control: AC-17.	
(2)	The organization requires that users of information system accounts, or roles, with access to administrative accounts, use non-privileged accounts, or roles, when accessing other system functions, and if feasible, audits any use of privileged accounts, or roles, for such functions.	
	Enhancement Supplemental Guidance: This control enhancement is intended to limit exposure due to operating from within a privileged account or role. The inclusion of role is intended to address those situations where an access control policy such as Role Based Access Control (RBAC) is being implemented and where a change of role provides the same degree of assurance in the change of access authorizations for both the user and all processes acting on behalf of the user as would be provided by a change between a privileged and non-privileged account. Audit of privileged activity may require physical separation employing information systems on which the user does not have privileged access.	
(5)	The organization limits authorization to super user accounts on the information system to designated system administration personnel.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: Super user accounts are typically described as “root” or “administrator” for various types of commercial off-the-shelf operating systems. Configuring organizational information systems (e.g., notebook/laptop computers, servers, workstations) such that day-to-day users are not authorized access to super user accounts is an example of limiting system authorization. The organization may differentiate in the application of this control enhancement between allowed privileges for local information system accounts and for domain accounts provided the organization retains the ability to control the configuration of the system with regard to key security parameters and as otherwise necessary to sufficiently mitigate risk.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.4 Description of groups, roles, and responsibilities for logical management of network components. 2.2.3 Configure system security parameters to prevent misuse 7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following: 7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities 7.1.2 Assignment of privileges is based on individual personnel’s job classification and function 7.1.3 Requirement for a documented approval by authorized parties specifying required privileges. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user’s need to know, and is set to “deny all” unless specifically allowed. 7.2.2 Assignment of privileges to individuals based on job classification and function. 12.5.5 Monitor and control all access to data.	
AC-7	**UNSUCCESSFUL LOGIN ATTEMPTS**	Previous SEC 501-06 Control References: 5.3.2.22
	Control: The information system:	
a.	Enforces a limit of 6 consecutive invalid access attempts by a user during a 15-minute time period; and	
b.	Automatically locks the account/node for a 30-minute period when the maximum number of unsuccessful attempts is exceeded. The control applies regardless of whether the login occurs via a local or network connection.	
	Supplemental Guidance: Due to the potential for denial of service, automatic lockouts initiated by the information system are usually temporary and automatically release after a predetermined time period established by the organization. If a delay algorithm is selected, the organization may chose to employ different algorithms for different information system components based on the capabilities of those components. Response to unsuccessful login attempts may be implemented at both the operating system and the application levels. This control applies to all accesses other than those accesses explicitly identified and documented by the organization in AC-14.	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(1)	The information system automatically locks the account/node until released by an administrator when the maximum number of unsuccessful attempts is exceeded.	
(2)	The information system provides additional protection for mobile devices accessed via login by purging information from the device after not more than ten consecutive, unsuccessful login attempts to the device.	
	Enhancement Supplemental Guidance: This enhancement applies only to mobile devices for which a login occurs (e.g., personal digital assistants) and not to mobile devices accessed without a login such as removable media. In certain situations, this enhancement may not apply to mobile devices if the information on the device is encrypted with sufficiently strong encryption mechanisms, making purging unnecessary. The login is to the mobile device, not to any one account on the device. Therefore, a successful login to any account on the mobile device resets the unsuccessful login count to zero.	
	DMV-Specific Requirements: Limit repeated access attempts by locking out the user ID after not more than six attempts during a 15-minute time period. PCI 8.5.13 VITA AC-7 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID. The control applies regardless of whether the login occurs via a local or network connection. PCI 8.5.14 VITA AC-7	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts. 8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	
AC-8	**SYSTEM USE NOTIFICATION**	Previous SEC 501-06 Control References: 8.4.2.3
	Control: The information system:	
a.	Displays an approved system use notification message or banner before granting access to the system that provides privacy and security notices consistent with applicable laws, directives, policies, regulations, standards, and guidance and states that: (i) users are accessing a Commonwealth of Virginia information system; (ii) system usage may be monitored, recorded, and subject to audit; (iii) unauthorized use of the system is prohibited and subject to criminal and civil penalties; and (iv) use of the system indicates consent to monitoring and recording;	
b.	Retains the notification message or banner on the screen until users take explicit actions to log on to or further access the information system; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
c.	For publicly accessible systems: (i) displays the system use information when appropriate, before granting further access; (ii) displays references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and (iii) includes in the notice given to public users of the information system, a description of the authorized uses of the system.	
	Supplemental Guidance: System use notification messages can be implemented in the form of warning banners displayed when individuals log in to the information system. System use notification is intended only for information system access that includes an interactive login interface with a human user and is not intended to require notification when an interactive interface does not exist.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AC-8-COV	**SYSTEM USE NOTIFICATION (COV)**	Previous SEC 501-06 Control References: 8.4.2.4
	Control: 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.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AC-10	**CONCURRENT SESSION CONTROL**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system limits the number of concurrent sessions for each system account to three sessions.	
	Supplemental Guidance: The organization may define the maximum number of concurrent sessions for an information system account globally, by account type, by account, or a combination. This control addresses concurrent sessions for a given information system account and does not address concurrent sessions by a single user via multiple system accounts.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AC-11	**SESSION LOCK**	Previous SEC 501-06 Control References: 4.7.2.6/5.4.2.7/5.3.2.18
	Control: The information system:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Prevents further access to the system by initiating a session lock after a maximum of 15 minutes of inactivity or upon receiving a request from a user; and	
b.	Retains the session lock until the user reestablishes access using established identification and authentication procedures.	
	Supplemental Guidance: A session lock is a temporary action taken when a user stops work and moves away from the immediate physical vicinity of the information system but does not want to log out because of the temporary nature of the absence. The session lock is implemented at the point where session activity can be determined. This is typically at the operating system-level, but may be at the application-level. A session lock is not a substitute for logging out of the information system, for example, if the organization requires users to log out at the end of the workday.	
	Control Enhancements for Sensitive Systems:	
(1)	The information system session lock mechanism, when activated on a device with a display screen, places a publically viewable pattern onto the associated display, hiding what was previously visible on the screen.	
	DMV-Specific Requirements: Implement a screen saver lockout period after a maximum of 15 minutes of inactivity for COV devices and require the user to re-authenticate to re-activate the terminal or session. PCI 8.5.15 VITA AC-11	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	
AC-14	**PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION**	Previous SEC 501-06 Control References: None
	DMV-Specific Requirements: VITA AC-14 DMV has withdrawn the control AC-14 although VITA SEC501-07 has not; DMV prohibits unauthenticated access to Agency information systems. DMV's prohibition on unauthenticated access complies with PCI 12.3.2	
	PCI compliance: PCI-DSS does not allow for exceptions to authenticating users: 12.3.2 Authentication for use of the technology.	
AC-17	**REMOTE ACCESS**	Previous SEC 501-06 Control References: 5.4.2.3c/5.4.2.6
	Control: The organization:	
a.	Documents allowed methods of remote access to the information system;	
b.	Establishes usage restrictions and implementation guidance for each allowed remote access method;	
c.	Monitors for unauthorized remote access to the information system;	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
d.	Authorizes remote access to the information system prior to connection; and	
e.	Enforces requirements for remote connections to the information system.	
	Supplemental Guidance: This control requires explicit authorization prior to allowing remote access to an information system without specifying a specific format for that authorization. For example, while the organization may deem it appropriate to use a system interconnection agreement to authorize a given remote access, such agreements are not required by this control. Remote access is any access to an organizational information system by a user (or process acting on behalf of a user) communicating through an external network (e.g., the Internet). Examples of remote access methods include dial-up, broadband, and wireless (see AC-18 for wireless access). A virtual private network when adequately provisioned with appropriate security controls, is considered an internal network (i.e., the organization establishes a network connection between organization controlled endpoints in a manner that does not require the organization to depend on external networks to protect the confidentiality or integrity of information transmitted across the network). Remote access controls are applicable to information systems other than public web servers or systems specifically designed for public access. Enforcing access restrictions associated with remote connections is accomplished by control AC-3. Related controls: AC-3, AC-18, AC-20, IA-2, IA-3, IA-8, MA-4.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs automated mechanisms to facilitate the monitoring and control of remote access methods.	
	Enhancement Supplemental Guidance: Automated monitoring of remote access sessions allows organizations to audit user activities on a variety of information system components (e.g., servers, workstations, notebook/laptop computers) and to ensure compliance with remote access policy.	
(2)	The organization uses cryptography to protect the confidentiality and integrity of remote access sessions.	
	Enhancement Supplemental Guidance: The encryption strength of mechanism is selected based on the security categorization of the information. Related controls: SC-8, SC-9, SC-13.	
(3)	The information system routes all remote accesses through a limited number of managed access control points.	
	Enhancement Supplemental Guidance: Related control: SC-7.	
(4)	The organization authorizes the execution of privileged commands and access to security-relevant information via remote access only for compelling operational needs and documents the rationale for such access in the security plan for the information system.	
	Enhancement Supplemental Guidance: Related control: AC-6.	
(5)	The organization monitors for unauthorized remote connections to the information system, and takes appropriate action if an unauthorized connection is discovered.	
(6)	The organization ensures that users protect information about remote access mechanisms from unauthorized use and disclosure.	
(7)	The organization ensures that remote sessions for accessing sensitive data or development environments employ two-factor authentication and are audited.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: Additional security measures are typically above and beyond standard bulk or session layer encryption (e.g., Secure Shell [SSH], Virtual Private Networking [VPN] with blocking mode enabled). Related controls: SC-8, SC-9.	
(8)	The organization disables all TCP and UDP ports except for explicitly identified components in support of specific operational requirements.	
	Enhancement Supplemental Guidance: The organization can either make a determination of the relative security of the networking protocol or base the security decision on the assessment of other entities. Bluetooth and peer-to-peer networking are examples of less than secure networking protocols.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) 8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	
AC-17-COV	**REMOTE ACCESS (COV)**	Previous SEC 501-06 Control References: 5.4.2
	Control: 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.	
	Supplemental Guidance: Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. Require maintenance of auditable records of all remote access. PCI 8.3 VITA AC-17	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
AC-18	**WIRELESS ACCESS**	Previous SEC 501-06 Control References: 4.8.2.1
	Control: The organization:	
a.	Establishes usage restrictions and implementation guidance for wireless access;	
b.	Monitors for unauthorized wireless access to the information system;	
c.	Authorizes wireless access to the information system prior to connection; and	
d.	Enforces requirements for wireless connections to the information system.	
	Supplemental Guidance: Wireless technologies include, but are not limited to, microwave, satellite, packet radio (UHF/VHF), 802.11x, and Bluetooth. Wireless networks use authentication protocols (e.g., EAP/TLS, PEAP), which provide credential protection and mutual authentication. In certain situations, wireless signals may radiate beyond the confines and control of organization controlled facilities. Related controls: AC-3, IA-2, IA-3, IA-8.	
	Control Enhancements for Sensitive Systems:	
(1)	The information system protects wireless access to the system using authentication and encryption.	
	Enhancement Supplemental Guidance: Authentication applies to user, device, or both as necessary. Related control: SC-13.	
(2)	The organization monitors for unauthorized wireless connections to the information system, including scanning for unauthorized wireless access points, and takes appropriate action if an unauthorized connection is discovered.	
	Enhancement Supplemental Guidance: Organizations proactively search for unauthorized wireless connections including the conduct of thorough scans for unauthorized wireless access points. The scan is not necessarily limited to only those areas within the facility containing the information systems, yet is conducted outside of those areas only as needed to verify that unauthorized wireless access points are not connected to the system.	
(3)	The organization disables, when not intended for use, wireless networking capabilities internally embedded within information system components prior to issuance and deployment.	
(4)	The organization does not allow users to independently configure wireless networking capabilities.	
	Enhancement Supplemental Guidance (COV): Wireless capabilities include the access points, authentication controllers, antennae, etc. Not to include client software on desktops or laptops. No ad-hoc mode.	
	DMV-Specific Requirements: Scanning for unauthorized wireless connections and wireless access points shall be done every three months. PCI 11.1 VITA AC-18	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. WEP encryption is not permitted. 11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis.	
AC-18-COV	**WIRELESS ACCESS (COV)**	Previous SEC 501-06 Control References: 4.8.2
	Control: Each agency ISO is accountable for ensuring the following steps are followed and documented:	
	Wireless LAN (WLAN) Connectivity on the COV Network	
1	The following requirements shall be met in the deployment, configuration and administration of WLAN infrastructure connected to any internal Commonwealth of Virginia network.	
a.	Client devices connecting to the WLAN must utilize two-factor authentication (i.e., digital certificates);	
b.	WLAN infrastructure must authenticate each client device prior to permitting access to the WLAN;	
c.	LAN user authorization infrastructure (i.e., Active Directory) must be used to authorize access to LAN resources;	
d.	Only COV owned or leased equipment shall be granted access to an internal WLAN;	
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);	
f.	Physical or logical separation between WLAN and wired LAN segments must exist;	
g.	All COV WLAN access and traffic must be monitored for malicious activity, and associated event log files stored on a centralized storage device;	
h.	Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and	
i.	WLAN clients will only permit infrastructure mode communication.	
	WLAN Hotspot (Wireless Internet)	
1	When building a wireless network, which will only provide unauthenticated access to the Internet, the following must be in place:	
a.	WLAN Hotspots must have logical or physical separation from the agency's LAN;	
b.	WLAN Hotspots must have packet filtering capabilities enabled to protect clients from malicious activity;	
c.	All WLAN Hotspot access and traffic must be monitored for malicious activity, and log files stored on a centralized storage device; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
d.	Where COV clients are concerned, WLAN clients will only permit infrastructure mode communication.	
	Wireless Bridging	
1	The following network configuration shall be used when bridging two wired LANs:	
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);	
b.	Wireless bridging devices will not have a default gateway configured;	
c.	Wireless bridging devices must be physically or logically separated from other networks;	
d.	Wireless bridge devices must only permit traffic destined to traverse the bridge and should not directly communicate with any other network;	
e.	Configuration and security data associated with the WLAN must not be provided to unauthenticated devices. For example, SSID broadcasting will be disabled; and	
f.	Wireless bridging devices must not be configured for any other service than bridging (i.e., a wireless access point).	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment. 2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings. 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. WEP encryption is not permitted.	
AC-19	**ACCESS CONTROL FOR MOBILE DEVICES**	Previous SEC 501-06 Control References: 5.3.2.1
	Control: The organization:	
a.	Establishes usage restrictions and implementation guidance for organization-controlled mobile devices;	
b.	Authorizes connection of mobile devices meeting organizational usage restrictions and implementation guidance to organizational information systems;	
c.	Monitors for unauthorized connections of mobile devices to organizational information systems;	
d.	Enforces requirements for the connection of mobile devices to organizational information systems;	
e.	Disables information system functionality that provides the capability for automatic execution of code on mobile devices without user direction;	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
f.	Issues specially configured mobile devices to individuals traveling to locations that the organization deems to be of significant risk in accordance with organizational policies and procedures; and	
g.	The following measures apply to mobile devices returning from locations likely to compromise the device's security, based on the judgment of the ISO/IT Security Office: 1. Before using, the device owner will deliver it to the IT Security Office. 2. The IT Security Office will assess the device based on the risk presented (e.g., where you traveled, what you did, which remote systems were accessed). 3. As part of the assessment the IT Security Office will compare the system to the baseline information captured and documented prior to the trip. This could include software state, hardware state and serial numbers (including internal components in some cases), and all access details for remote-access systems. Depending on the sensitivity of data the system had access to, the location visited and the risk assessment of the inspecting staff, wiping the device clean and reinstalling it, or in some cases, even discarding the device may be required.	
	Supplemental Guidance: Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). Organization-controlled mobile devices include those devices for which the organization has the authority to specify and the ability to enforce specific security requirements. Usage restrictions and implementation guidance related to mobile devices include, for example, configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared). Examples of information system functionality that provide the capability for automatic execution of code are AutoRun and AutoPlay. Organizational policies and procedures for mobile devices used by individuals departing on and returning from travel include, for example, determining which locations are of concern, defining required configurations for the devices, ensuring that the devices are configured as intended before travel is initiated, and applying specific measures to the device after travel is completed. Specially configured mobile devices include, for example, computers with sanitized hard drives, limited applications, and additional hardening (e.g., more stringent configuration settings). Specified measures applied to mobile devices upon return from travel include, for example, examining the device for signs of physical tampering and purging/reimaging the hard disk drive. Protecting information residing on mobile devices is covered in the media protection family. Related controls: MP-4, MP-5.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization restricts the use of writable, removable media in organizational information systems .	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(2)	The organization prohibits the use of personally owned, removable media in organizational information systems.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	
AC-20	**USE OF EXTERNAL INFORMATION SYSTEMS**	Previous SEC 501-06 Control References: 8.4.2.5/6.2.2.3
	Control: The organization establishes terms and conditions, consistent with any trust relationships established with other organizations owning, operating, and/or maintaining external information systems, allowing authorized individuals to:	
a.	Access the information system from the external information systems; and	
b.	Process, store, and/or transmit organization-controlled information using the external information systems.	
	Supplemental Guidance: External information systems are information systems or components of information systems that are outside of the authorization boundary established by the organization and for which the organization typically has no direct supervision and authority over the application of required security controls or the assessment of security control effectiveness. External information systems include, but are not limited to: (i) personally owned information systems (e.g., computers, cellular telephones, or personal digital assistants); (ii) privately owned computing and communications devices resident in commercial or public facilities (e.g., hotels, convention centers, or airports); The organization establishes terms and conditions for the use of external information systems in accordance with organizational security policies and procedures. The terms and conditions address as a minimum; (i) the types of applications that can be accessed on the organizational information system from the external information system; and (ii) the maximum security categorization of information that can be processed, stored, and transmitted on the external information system. This control defines access authorizations enforced by AC-3, rules of behavior requirements enforced by PL-4, and session establishment rules enforced by AC-17. Related controls: AC-3, AC-17, PL-4.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization permits authorized individuals to use an external information system to access the information system or to process, store, or transmit organization-controlled information only when the organization:	
(a)	Can verify the implementation of required security controls on the external system as specified in the organization's information security policy and security plan; or	
(b)	Has approved information system connection or processing agreements with the organizational entity hosting the external information system.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(2)	The organization limits the use of organization-controlled portable storage media by authorized individuals on external information systems.	
	Enhancement Supplemental Guidance: Limits on the use of organization-controlled portable storage media in external information systems can include, for example, complete prohibition of the use of such devices or restrictions on how the devices may be used and under what conditions the devices may be used.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following: 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	
AC-20-COV	**USE OF EXTERNAL INFORMATION SYSTEMS (COV)**	Previous SEC 501-06 Control References: 10.2.2.2
	Control: 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.	
	1. Non-COV computers, smart phones, etc. shall not be directly connected to the COV network. 2. The exception to 1. above is for vendors who provide direct support for IT systems. a. In these cases there should be a documented business need and the approval of the ISO. b. The vendor is responsible for ensuring that appropriate operating system, security software, and virus updates and patches are applied at regular interval to the equipment used to access the network. 3. On-site vendors may connect to an established vendor network. a. In these cases there should be a documented business need and the approval of the ISO. b. The vendor is responsible for ensuring that appropriate operating system, security software, and virus updates and patches are applied at regular interval to the equipment used to access the network.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
AC-21	**USER-BASED COLLABORATION AND INFORMATION SHARING**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization:	
a.	Facilitates information sharing by enabling authorized users to determine whether access authorizations assigned to the sharing partner match the access restrictions on the information.	
	Supplemental Guidance: The control applies to information that may be restricted in some manner (e.g., privileged medical, contract-sensitive, proprietary, personally identifiable information, special access programs/compartments) based on some formal or administrative determination. Depending on the information-sharing circumstance, the sharing partner may be defined at the individual, group, or organization level and information may be defined by specific content, type, or security categorization. Related control: AC-3.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AC-22	**PUBLICLY ACCESSIBLE CONTENT**	Previous SEC 501-06 Control References: 2.4.2.8
	Control: The organization:	
a.	Designates individuals authorized to post information onto an organizational information system that is publicly accessible;	
b.	Trains authorized individuals to ensure that publicly accessible information does not contain nonpublic information;	
c.	Reviews the proposed content of publicly accessible information for nonpublic information prior to posting onto the organizational information system;	
d.	Reviews the content on the publicly accessible organizational information system for nonpublic information every 60-days at a minimum and	
e.	Removes nonpublic information from the publicly accessible organizational information system, if discovered.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Nonpublic information is any information for which the general public is not authorized access in accordance with laws, directives, policies, regulations, standards, or guidance. Information protected under the Privacy Act and vendor proprietary information are examples of nonpublic information. This control addresses posting information on an organizational information system that is accessible to the general public, typically without identification or authentication. The posting of information on non-organization information systems is covered by appropriate organizational policy. Related controls: AC-3, AU-13.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
2.2	***FAMILY:*** *AWARENESS AND TRAINING*	***CLASS:*** *OPERATIONAL*
AT-2	**SECURITY AWARENESS**	Previous SEC 501-06 Control References: 8.3.2.2
	Control: The organization provides basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and annually or more often as necessary thereafter.	
	Supplemental Guidance: The content includes a basic understanding of the need for information security and user actions to maintain security and to respond to suspected security incidents. The content also addresses awareness of the need for operations security as it relates to the organization's information security program. Security awareness techniques can include, for example, displaying posters, offering supplies inscribed with security reminders, generating email advisories/notices from senior organizational officials, displaying logon screen messages, and conducting information security awareness events.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data. 12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. 12.6.1 Educate personnel upon hire at least annually.	
AT-2-COV	**SECURITY AWARENESS (COV)**	Previous SEC 501-06 Control References: 8.3.2.6/8.3.2.7
1	**Control: Develop an information 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 information security incidents, including those caused by malicious code;	
d.	Proper disposal of data storage media;	
e.	Proper use of encryption;	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
f.	Access controls, including creating and changing passwords and the need to keep them confidential;	
g.	Agency acceptable use policies;	
h.	Agency Remote Access policies; and	
i.	Intellectual property rights, including software licensing and copyright issues.	
j.	Responsibility for the security of COV data;	
k.	Phishing; and	
l.	Social engineering.	
2	Require documentation of IT system users' acceptance of the agency's security policies after receiving information security training.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data. 12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security. 12.6.1 Educate personnel upon hire at least annually. 12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	
AT-3	**SECURITY TRAINING**	Previous SEC 501-06 Control References: 8.3.2.2/8.2.2.3
	Control: The organization provides role-based security-related training: (i) before authorizing access to the system or performing assigned duties; (ii) when required by system changes; and (iii) as practical and necessary thereafter.	
	Supplemental Guidance: The organization determines the appropriate content of security training based on assigned roles and responsibilities and the specific requirements of the organization and the information systems to which personnel have authorized access. In addition, the organization provides information system managers, system and network administrators, personnel performing independent verification and validation activities, security control assessors, and other personnel having access to system-level software, adequate security-related technical training to perform their assigned duties. Organizational security training addresses management, operational, and technical roles and responsibilities covering physical, personnel, and technical safeguards and countermeasures. The organization also provides the training necessary for these individuals to carry out their responsibilities related to operations security within the context of the organization's information security program. Related controls: AT-2, SA-3 .	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
AT-4	**SECURITY TRAINING RECORDS**	Previous SEC 501-06 Control References: 8.3.2.5
	Control: The organization:	
a.	Documents and monitors individual information system security training activities including basic security awareness training and specific information system security training; and	
b.	Retains individual training records for 3 years after completion of training then destroy.	
	Supplemental Guidance: While an organization may deem that organizationally mandated individual training programs and the development of individual training plans are necessary, this control does not mandate either. Documentation for specialized training may be maintained by individual supervisors at the option of the organization. Library of Virginia **Schedule GS-103: Personnel Records**, *Training Records Not Required for Certification or Qualification,* series 100501 - specifies 3 year retention for employee training records.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AT-5	**CONTACTS WITH SECURITY GROUPS AND ASSOCIATIONS**	Previous SEC 501-06 Control References: 9.2.2.5
	Control: The organization establishes and institutionalizes contact with selected groups and associations within the security community:	
	To facilitate ongoing security education and training for organizational personnel;	
	To stay up to date with the latest recommended security practices, techniques, and technologies; and	
	To share current security-related information including threats, vulnerabilities, and incidents.	
	Supplemental Guidance: Ongoing contact with security groups and associations is of paramount importance in an environment of rapid technology changes and dynamic threats. Security groups and associations can include, for example, special interest groups, specialized forums, professional associations, news groups, and/or peer groups of security professionals in similar organizations. The groups and associations selected are consistent with the organization's mission/business requirements. Information-sharing activities regarding threats, vulnerabilities, and incidents related to information systems are consistent with applicable laws, directives, policies, regulations, standards, and guidance.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
2.3	***FAMILY:*** *AUDIT AND ACCOUNTABILITY*	***CLASS:*** *TECHNICAL*
AU-2	**AUDITABLE EVENTS**	Previous SEC 501-06 Control References: 9.3.2.2
	Control: The organization:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: authenticated individual, access time, source of access, duration of access, and actions executed	
b.	Coordinates the security audit function with other organizational entities requiring audit related information to enhance mutual support and to help guide the selection of auditable events;	
c.	Provides a rationale for why the list of auditable events are deemed to be adequate to support after-the-fact investigations of security incidents; and	
d.	Determines, based on current threat information and ongoing assessment of risk, that the following events are to be audited within the information system: authenticated individual, access time, source of access, and actions executed	
	Supplemental Guidance: The purpose of this control is for the organization to identify events which need to be auditable as significant and relevant to the security of the information system; giving an overall system requirement in order to meet ongoing and specific audit needs. To balance auditing requirements with other information system needs, this control also requires identifying that subset of auditable events that are to be audited at a given point in time. For example, the organization may determine that the information system must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the extreme burden on system performance. In addition, audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the right level of abstraction for audit record generation is a critical aspect of an audit capability and can facilitate the identification of root causes to problems. Related control: AU-3.	
	Control Enhancements for Sensitive Systems:	
(3)	The organization reviews and updates the list of auditable events once a year at a minimum.	
	Enhancement Supplemental Guidance: The list of auditable events is defined in AU-2.	
(4)	The organization includes execution of privileged functions in the list of events to be audited by the information system.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data. 10.2.2 All actions taken by any individual with root or administrative privileges. 10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification. 10.3.2 Type of event. 10.3.3 Date and time. 10.3.4 Success or failure indication. 10.3.5 Origination of event. 10.3.6 Identity or name of affected data, system component, or resource.	
AU-3	**CONTENT OF AUDIT RECORDS**	Previous SEC 501-06 Control References: 9.3.2.2

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.	
	Supplemental Guidance: Audit record content that may be necessary to satisfy the requirement of this control, includes, for example, time stamps, source and destination addresses, user/process identifiers, event descriptions, success/fail indications, filenames involved, and access control or flow control rules invoked. Related controls: AU-2, AU-8.	
	Control Enhancements for Sensitive Systems:	
(1)	The information system may include additional organization defined requirements in the audit records for audit events identified by type, location, or subject.	
	Enhancement Supplemental Guidance: An example of detailed information that the organization may require in audit records is full-text recording of privileged commands or the individual identities of group account users.	
(2)	The organization centrally manages the content of audit records generated by all web servers, database servers, messaging servers, file servers, print servers, middleware servers, dns servers, routers, firewalls, IDS/IPS, and VoIP servers.	
	DMV-Specific Requirements: DMV requires audit records/logs to be stored and managed on server(s) on an internal network segment. PCI 10.5.4 VITA AU-3	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data. 10.2.2 All actions taken by any individual with root or administrative privileges. 10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification. 10.3.2 Type of event. 10.3.3 Date and time. 10.3.4 Success or failure indication. 10.3.5 Origination of event. 10.3.6 Identity or name of affected data, system component, or resource. 10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.	
AU-4	**AUDIT STORAGE CAPACITY**	Previous SEC 501-06 Control References: None
	Control: The organization allocates audit record storage capacity and configures auditing to reduce the likelihood of such capacity being exceeded.	
	Supplemental Guidance: The organization considers the types of auditing to be performed and the audit processing requirements when allocating audit storage capacity. Related controls: AU-2, AU-5, AU-6, AU-7, SI-4.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
AU-5	**RESPONSE TO AUDIT PROCESSING FAILURES**	Previous SEC 501-06 Control References: None
	Control: The information system:	
a.	Alerts designated organizational officials in the event of an audit processing failure; and	
	Supplemental Guidance: Audit processing failures include, for example, software/hardware errors, failures in the audit capturing mechanisms, and audit storage capacity being reached or exceeded. Related control: AU-4.	
	Control Enhancements for Sensitive Systems:	
(2)	The information system provides a real-time alert when the following audit failure events occur: recording of authentication attempts, modification of sensitive data, or escalation of privilege.	
	PCI compliance: PCI-DSS has no requirement for this control.	
AU-6	**AUDIT REVIEW, ANALYSIS, AND REPORTING**	Previous SEC 501-06 Control References: None
	Control: The organization:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Reviews and analyzes information system audit records at least every 30-days at a minimum for indications of inappropriate or unusual activity, and reports findings to designated organizational officials; and	
b.	Adjusts the level of audit review, analysis, and reporting within the information system when there is a change in risk to organizational operations, organizational assets, individuals, other organizations, or the Commonwealth based on law enforcement information, intelligence information, or other credible sources of information.	
	Supplemental Guidance: Related control: AU-7.	
	Control Enhancements for Sensitive Systems:	
(1)	The information system integrates audit review, analysis, and reporting processes to support organizational processes for investigation and response to suspicious activities.	
(3)	The organization analyzes and correlates audit records across different repositories to gain organization-wide situational awareness.	
(4)	The information system centralizes the review and analysis of audit records from multiple components within the system.	
	Enhancement Supplemental Guidance: An example of an automated mechanism for centralized review and analysis is a Security Information Management (SIM) product. Related control: AU-2.	
(5)	The organization integrates analysis of audit records with analysis of vulnerability scanning information, performance data, and network monitoring information to further enhance the ability to identify inappropriate or unusual activity.	
	Enhancement Supplemental Guidance: A Security Event/Information Management system tool can facilitate audit record aggregation and consolidation from multiple information system components as well as audit record correlation and analysis. The use of standardized audit record analysis scripts developed by the organization (with localized script adjustments, as necessary), provides a more cost-effective approach for analyzing audit record information collected. The correlation of audit record information with vulnerability scanning information is important in determining the veracity of the vulnerability scans and correlating attack detection events with scanning results. Related control: AU-7, RA-5, SI-4.	
	PCI compliance: 10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS). **NOTE:** The requirement for daily log review (PCI 10.6) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control AU-6's requirements apply to all other DMV systems.	
AU-8	**TIME STAMPS**	Previous SEC 501-06 Control References: 9.3.2.2
	Control: The information system uses internal system clocks to generate time stamps for audit records.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Time stamps generated by the information system include both date and time. The time may be expressed in Coordinated Universal Time (UTC), a modern continuation of Greenwich Mean Time (GMT), or local time with an offset from UTC. Related control: AU-3.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time. 10.4.1 Critical systems have the correct and consistent time. 10.4.3 Time settings are received from industry-accepted time sources.	
AU-9	**PROTECTION OF AUDIT INFORMATION**	Previous SEC 501-06 Control References: None
	Control: The information system protects audit information and audit tools from unauthorized access, modification, and deletion.	
	Supplemental Guidance: Audit information includes all information (e.g., audit records, audit settings, and audit reports) needed to successfully audit information system activity. Related controls: AC-3, AC-6.	
	Control Enhancements for Sensitive Systems:	
(2)	The information system backs up audit records at least once every twenty-four hours onto a different system or media than the system being audited.	
(4)	The organization:	
(a)	Authorizes access to management of audit functionality to only a limited subset of privileged users; and	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 10.4.2 Time data is protected. 10.5 Secure audit trails so they cannot be altered. 10.5.1 Limit viewing of audit trails to those with a job-related need. 10.5.2 Protect audit trail files from unauthorized modifications. 10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	
AU-11	**AUDIT RECORD RETENTION**	Previous SEC 501-06 Control References: None
	Control: The organization retains audit records consistent with the Agency's records retention policy to provide support for after-the-fact investigations of security incidents and to meet regulatory and organizational information retention requirements.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The organization retains audit records until it is determined that they are no longer needed for administrative, legal, audit, or other operational purposes. This includes, for example, retention and availability of audit records relative to Freedom of Information Act (FOIA) requests, subpoena, and law enforcement actions. Standard categorizations of audit records relative to such types of actions and standard response processes for each type of action are developed and disseminated. The Library of Virginia and the Payment Card Industry Data Security Standard (PCI-DSS) provide the policy on records retention. DMV will comply with the most restrictive requirements of these two sources.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	
AU-12	**AUDIT GENERATION**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system:	
a.	Provides audit record generation capability for the list of auditable events defined in AU-2.	
b.	Allows designated organizational personnel to select which auditable events are to be audited by specific components of the system; and	
c.	Generates audit records for the list of audited events defined in AU-2 with the content as defined in AU-3.	
	Supplemental Guidance: Audit records can be generated from various components within the information system. The list of audited events is the set of events for which audits are to be generated. This set of events is typically a subset of the list of all events for which the system is capable of generating audit records (i.e., auditable events). Related controls: AU-2, AU-3.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: Aligns generally with 10.1 & 10.2, but AU-12 AUDIT GENERATION must integrate with AU-2 AUDITABLE EVENTS and AU-3 CONTENT OF AUDIT RECORDS to fully meet PCI requirements.	
2.4	***FAMILY** : SECURITY ASSESSMENT AND AUTHORIZATION*	***CLASS:** MANAGEMENT*
CA-2	**SECURITY ASSESSMENTS**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization:	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	
(2)	The organization includes as part of security control assessments, at least once a year at a minimum, unannounced penetration testing of sensitive applications.	
	Enhancement Supplemental Guidance: Penetration testing exercises both physical and technical security controls. A standard method for penetration testing consists of: (i) pretest analysis based on full knowledge of the target system; (ii) pretest identification of potential vulnerabilities based on pretest analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenario. These rules of engagement are correlated with the tools, techniques, and procedures that are anticipated to be employed by threat-sources in carrying out attacks. An organizational assessment of risk guides the decision on the level of independence required for penetration agents or penetration teams conducting penetration testing. Red team exercises are conducted as a simulated adversarial attempt to compromise organizational missions and/or business processes to provide a comprehensive assessment of the security capability of the information system and organization. While penetration testing may be laboratory-based testing, red team exercises are intended to be more comprehensive in nature and reflect real-world conditions. Information system monitoring, malicious user testing, penetration testing, red-team exercises, and other forms of security testing (e.g., independent verification and validation) are conducted to improve the readiness of the organization by exercising organizational capabilities and indicating current performance levels as a means of focusing organizational actions to improve the security state of the system and organization. Testing is conducted in accordance with applicable laws, directives, policies, regulations, and standards. Testing methods are approved by authorizing officials in coordination with the organization's Risk Executive Function. Vulnerabilities uncovered during red team exercises are incorporated into the vulnerability remediation process. Related controls: RA-5, SI-2.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: 11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: 11.3.1 Network-layer penetration tests. 11.3.2 Application-layer penetration tests.	
CA-3	**INFORMATION SYSTEM CONNECTIONS**	Previous SEC 501-06 Control References: None
	Control: The organization:	
a.	Authorizes connections from the information system to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements;	
b.	Documents, for each connection, the interface characteristics, security requirements, and the nature of the information communicated; and	
c.	Monitors the information system connections on an ongoing basis verifying enforcement of security requirements.	
	Supplemental Guidance: This control applies to dedicated connections between information systems and does not apply to transitory, user-controlled connections such as email and website browsing. The organization carefully considers the risks that may be introduced when information systems are connected to other systems with different security requirements and security controls, both within the organization and external to the organization. Authorizing officials determine the risk associated with each connection and the appropriate controls employed. If the interconnecting systems have the same authorizing official, an Interconnection Security Agreement is not required. Rather, the interface characteristics between the interconnecting information systems are described in the security plans for the respective systems. If the interconnecting systems have different authorizing officials but the authorizing officials are in the same organization, the organization determines whether an Interconnection Security Agreement is required, or alternatively, the interface characteristics between systems are described in the security plans of the respective systems. Instead of developing an Interconnection Security Agreement, organizations may choose to incorporate this information into a formal contract, especially if the interconnection is to be established between a agency and a non-Commonwealth (private sector) organization. In every case, documenting the interface characteristics is required, yet the formality and approval process vary considerably even though all accomplish the same fundamental objective of managing the risk being incurred by the interconnection of the information systems. Risk considerations also include information systems sharing the same networks. Information systems may be identified and authenticated as devices in accordance with IA-3. Related controls: AC-4, IA-3, SC-7, SA-9.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following: 12.8.1 Maintain a list of service providers. 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	
CA-3-COV	**INFORMATION SYSTEM CONNECTIONS (COV)**	Previous SEC 501-06 Control References: 4.4.2
1	**Control: For every sensitive Agency IT system that shares data with non-Commonwealth entities, the Agency shall require or shall specify that its service provider require:**	
a.	The System Owner, in consultation with the Data Owner, shall document IT systems with which data is shared. This documentation must include:	
b.	The types of shared data;	
c.	The direction(s) of data flow; and	
d.	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.	
2	The System Owners of interconnected systems must inform one another of connections with other systems.	
3	The System Owners of interconnected systems must notify each other prior to establishing connections to other systems.	
4	The written agreement shall specify if and how the shared data will be stored on each IT system.	
5	The written agreement shall specify that System Owners of the IT systems that share data acknowledge and agree to abide by any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data, including but not limited to Data Breach requirements in this Standard.	
6	The written agreement shall specify each Data Owner's authority to approve access to the shared data.	
7	The System Owners shall approve and enforce the agreement.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following: 12.8.1 Maintain a list of service providers. 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	
CA-6	**SECURITY AUTHORIZATION**	Previous SEC 501-06 Control References: None
	Control: The organization:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Assigns a senior-level executive or manager to the role of authorizing official for the information system;	
b.	Ensures that the authorizing official authorizes the information system for processing before commencing operations; and	
c.	Updates the security authorization once a year at a minimum.	
	Supplemental Guidance: Security authorization is the official management decision, conveyed through the authorization decision document, given by a senior organizational official or executive (i.e., authorizing official) to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Commonwealth based on the implementation of an agreed-upon set of security controls. Authorizing officials typically have budgetary oversight for information systems or are responsible for the mission or business operations supported by the systems. Security authorization is an inherently Commonwealth responsibility and therefore, authorizing officials must be Commonwealth employees. Through the security authorization process, authorizing officials are accountable for the security risks associated with information system operations. Accordingly, authorizing officials are in management positions with a level of authority commensurate with understanding and accepting such information system-related security risks. Through the employment of a comprehensive continuous monitoring process, the critical information contained in the authorization package (i.e., the security plan (including risk assessment), the security assessment report, and the plan of action and milestones) is updated on an ongoing basis, providing the authorizing official and the	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
CA-7	**CONTINUOUS MONITORING**	Previous SEC 501-06 Control References: None
	Control: The organization establishes a continuous monitoring strategy and implements a continuous monitoring program that includes:	
a.	A configuration management process for the information system and its constituent components;	
b.	A determination of the security impact of changes to the information system and environment of operation;	
c.	Ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and	
d.	Reporting the security state of the information system to appropriate organizational officials every 120-days at a minimum.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: A continuous monitoring program allows an organization to maintain the security authorization of an information system over time in a highly dynamic environment of operation with changing threats, vulnerabilities, technologies, and missions/business processes. Continuous monitoring of security controls using automated support tools facilitates near real-time risk management and promotes organizational situational awareness with regard to the security state of the information system. The implementation of a continuous monitoring program results in ongoing updates to the security plan, the security assessment report, and the plan of action and milestones, the three principal documents in the security authorization package. A rigorous and well executed continuous monitoring program significantly reduces the level of effort required for the reauthorization of the information system. Continuous monitoring activities are scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-5, CA-6, CM-3, CM-4.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.4.5.1 Documentation of impact. 6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	
2.5	***FAMILY:*** *CONFIGURATION MANAGEMENT*	***CLASS:*** *OPERATIONAL*
CM-2	**BASELINE CONFIGURATION**	Previous SEC 501-06 Control References: 4.3.2.1
	Control: The organization develops, documents, and maintains under configuration control, a current baseline configuration of the information system.	
	Supplemental Guidance: This control establishes a baseline configuration for the information system and its constituent components including communications and connectivity-related aspects of the system. The baseline configuration provides information about the components of an information system (e.g., the standard software load for a workstation, server, network component, or mobile device including operating system/installed applications with current version numbers and patch information), network topology, and the logical placement of the component within the system architecture. The baseline configuration is a documented, up-to-date specification to which the information system is built. Maintaining the baseline configuration involves creating new baselines as the information system changes over time. The baseline configuration of the information system is consistent with the organization's enterprise architecture. Related controls: CM-3, CM-6, CM-8, CM-9.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization reviews and updates the baseline configuration of the information system:	
(a)	Once a year at a minmum;	
(b)	When required due to a significant configuration change or a demonstrated vulnerability; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(c)	As an integral part of information system component installations and upgrades.	
(5)	The organization:	
(a)	Develops and maintains a list of software programs authorized to execute on the information system; and	
(b)	Employs a deny-all, permit-by-exception authorization policy to identify software allowed to execute on the information system.	
(6)	The organization maintains a baseline configuration for development and test environments that is managed separately from the operational baseline configuration.	
	PCI requirements: 1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks. 1.1.6 Requirement to review firewall and router rule sets at least every six months. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. **NOTE:** The requirement for review of firewall and router rule sets every 6 months (PCI 1.1.6) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control CM-2's requirements apply to all other DMV systems.	
CM-2-COV	**BASELINE CONFIGURATION (COV)**	Previous SEC 501-06 Control References: 4.3.2
1	**Control: The organization:**	
a.	Identify, document, and apply more restrictive security configurations for sensitive Agency IT systems, as necessary.	
b.	Maintain records that document the application of baseline security configurations.	
c.	Monitor systems for security baselines and policy compliance.	
d.	Reapply all security configurations to IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.	
e.	Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.	
2	Require creation and periodic review of a list of agency hardware and software assets.	
3	The organization reviews and updates the baseline configuration of all information system:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Once a year at a minimum;	
b.	When required due to a significant configuration change or a demonstrated vulnerability; and	
c.	As an integral part of information system component installations and upgrades.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI requirements: 1.1.6 Requirement to review firewall and router rule sets at least every six months. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. And the Device list aspect of: 12.3.3 A list of all such devices and personnel with access. **NOTE:** The requirement for review of firewall and router rule sets every 6 months (PCI 1.1.6) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control CM-2-COV's requirements apply to all other DMV systems.	
CM-3	**CONFIGURATION CHANGE CONTROL**	Previous SEC 501-06 Control References: 10.4.1
	Control: The organization:	
a.	Determines the types of changes to the information system that are configuration controlled;	
b.	Approves configuration-controlled changes to the system with explicit consideration for security impact analyses;	
c.	Documents approved configuration-controlled changes to the system;	
d.	Retains and reviews records of configuration-controlled changes to the system;	
e.	Audits activities associated with configuration-controlled changes to the system; and	
f.	Coordinates and provides oversight for configuration change control activities through a Change Control Board that convenes on a regular basis to review changes prior to implementation.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The organization determines the types of changes to the information system that are configuration controlled. Configuration change control for the information system involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the system, including upgrades and modifications. Configuration change control includes changes to components of the information system, changes to the configuration settings for information technology products (e.g., operating systems, applications, firewalls, routers), emergency changes, and changes to remediate flaws. A typical organizational process for managing configuration changes to the information system includes, for example, a chartered Configuration Control Board that approves proposed changes to the system. Auditing of changes refers to changes in activity before and after a change is made to the information system and the auditing activities required to implement the change. Related controls: CM-4, CM-5, CM-6, SI-2.	
	Control Enhancements for Sensitive Systems:	
(2)	The organization tests, validates, and documents changes to the information system before implementing the changes on the operational system.	
	Enhancement Supplemental Guidance: The organization ensures that testing does not interfere with information system operations. The individual/group conducting the tests understands the organizational information security policies and procedures, the information system security policies and procedures, and the specific health, safety, and environmental risks associated with a particular facility and/or process. An operational system may need to be taken off-line, or replicated to the extent feasible, before testing can be conducted. If an information system must be taken off-line for testing, the tests are scheduled to occur during planned system outages whenever possible. In situations where the organization cannot conduct testing of an operational system, the organization employs compensating controls (e.g., providing a replicated system to conduct testing) in accordance with the general tailoring guidance.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: DMV's *Information Technology Change Management Policy and Procedures* details the steps to request, schedule, and implement changes, including required documentation: a. Description of Change b. Effect on Availability and Customer Impact Statement c. Risks d. Prerequisites e. Change Plan f. Backout Plan g. Test Plan h. Documentation Updates i. Relationship to Other Changes It also establishes a Change Control Board that meets weekly to review and approve/deny change requests; this Board requires attendance by representatives from all technical areas including IT Security. Please refer to DMV's ***IT Change Control Policy*** for complete details. PCI 6.4.5	
(4)	The organization requires an information security representative to be a member of the Change Control Board.	
	Enhancement Supplemental Guidance: Information security representatives can include, for example, information system security officers or information system security managers. The configuration change control element in this control enhancement is consistent with the change control element defined by the organization in CM-3.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations 6.4.5 Change control procedures for the implementation of security patches and software modifications. 6.4.5.1 Documentation of impact. 6.4.5.2 Documented change approval by authorized parties.	
CM-3-COV	**CONFIGURATION CHANGE CONTROL (COV)**	Previous SEC 501-06 Control References: 10.4.2
	Control: Each Agency shall, or shall require that its service provider, document and implement configuration management and change control practices so that changes to the IT environment do not compromise security controls.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.4.5 Change control procedures for the implementation of security patches and software modifications. 6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	
CM-4	**SECURITY IMPACT ANALYSIS**	Previous SEC 501-06 Control References: None
	Control: The organization analyzes changes to the information system to determine potential security impacts prior to change implementation.	
	Supplemental Guidance: Security impact analyses are conducted by organizational personnel with information security responsibilities, including for example, Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers. Individuals conducting security impact analyses have the appropriate skills and technical expertise to analyze the changes to information systems and the associated security ramifications. Security impact analysis may include, for example, reviewing information system documentation such as the security plan to understand how specific security controls are implemented within the system and how the changes might affect the controls. Security impact analysis may also include an assessment of risk to understand the impact of the changes and to determine if additional security controls are required. Security impact analysis is scaled in accordance with the security categorization of the information system. Related controls: CA-2, CA-7, CM-3, CM-9, SI-2.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization analyzes new software in a separate test environment before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or intentional malice.	
(2)	The organization, after the information system is changed, checks the security functions to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the security requirements for the system.	
	Enhancement Supplemental Guidance: Changes include information system upgrades and modifications.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: Change control procedures - 6.4.5.1 Documentation of impact. 6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	
CM-5	**ACCESS RESTRICTIONS FOR CHANGE**	Previous SEC 501-06 Control References: None

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control: The organization defines, documents, approves, and enforces physical and logical access restrictions associated with changes to the information system.	
	Supplemental Guidance: Any changes to the hardware, software, and/or firmware components of the information system can potentially have significant effects on the overall security of the system. Accordingly, only qualified and authorized individuals are allowed to obtain access to information system components for purposes of initiating changes, including upgrades and modifications. Additionally, maintaining records of access is essential for ensuring that configuration change control is being implemented as intended and for supporting after-the-fact actions should the organization become aware of an unauthorized change to the information system. Access restrictions for change also include software libraries. Examples of access restrictions include, for example, physical and logical access controls (see AC-3 and PE-3), workflow automation, media libraries, abstract layers (e.g., changes are implemented into a third-party interface rather than directly into the information system component), and change windows (e.g., changes occur only during specified times, making unauthorized changes outside the window easy to discover). Some or all of the enforcement mechanisms and processes necessary to implement this security control are included in other controls. For measures implemented in other controls, this control provides information to be used in the implementation of the other controls to cover specific needs related to enforcing authorizations to make changes to the information system, auditing changes, and retaining and review records of changes. Related controls: AC-3, AC-6, PE-3.	
	Control Enhancements for Sensitive Systems:	
(5)	The organization:	
(a)	Limits information system developer/integrator privileges to change hardware, software, and firmware components and system information directly within a production environment; and	
(b)	Reviews and reevaluates information system developer/integrator privileges annually.	
	PCI compliance: PCI-DSS has no requirement for this control.	
CM-6	**CONFIGURATION SETTINGS**	Previous SEC 501-06 Control References: 4.3.2
	Control: The organization:	
a.	Establishes and documents mandatory configuration settings for information technology products employed within the information system using the Commonwealth of Virginia System Hardening Standard that reflect the most restrictive mode consistent with operational requirements;	
b.	Implements the configuration settings;	
c.	Identifies, documents, and approves exceptions from the mandatory configuration settings for individual components within the information system based on explicit operational requirements; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
d.	Monitors and controls changes to the configuration settings in accordance with organizational policies and procedures.	
	Supplemental Guidance: Configuration settings are the configurable security-related parameters of information technology products that are part of the information system. Security-related parameters are those parameters impacting the security state of the system including parameters related to meeting other security control requirements. Security-related parameters include, for example, registry settings; account, file, and directory settings (i.e., permissions); and settings for services, ports, protocols, and remote connections. Organizations establish organization-wide mandatory configuration settings from which the settings for a given information system are derived. A security configuration checklist (sometimes referred to as a lockdown guide, hardening guide, security guide, security technical implementation guide [STIG], or benchmark) is a series of instructions or procedures for configuring an information system component to meet operational requirements. Checklists can be developed by information technology developers and vendors, consortia, academia, industry, Commonwealth agencies (and other government organizations), and others in the public and private sectors. Related controls: CM-2, CM-3, SI-4.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. 2.2.2 Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. 2.2.3 Configure system security parameters to prevent misuse 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	
CM-7	**LEAST FUNCTIONALITY**	Previous SEC 501-06 Control References: None
	Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services that are not required for the business function of the information system.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: DMV configures the information system based on the security principles of “Least Privilege”. The security model employed is based on best practices published by the NSA, NIST, Center for Internet Security and accredited security organizations such as ISC2 and SANS. These defined security models are applied to workstation, servers, applications and other elements of the infrastructure. 1. DMV does not allow direct connections from outside sources to internal systems. 2. DMV requires multi-level security models for risk minimization. 3. All externally and most internally available applications are designed in a multi-tier security model. The tiers are hosted on separate hardware resources and are separated by independent firewalls. These are not application layers but independent operational tiers that only can communicate with one another in distinct and prescribed ways. 4. No http proxy based applications are allowed. 5. DMV restricts the IP application ports that are allowed to traverse networks and segments. It should not be assumed by an application has access to any port unless this security architecture policy specifically describes such interaction. 6. DMV does not allow dynamic port allocation applications. 7. DMV considers any machine that is directly accessed by an outside entity as a perimeter device and restricts accordingly. 8. DMV does not allow the sharing of security credentials for user access to DMV systems. This includes both DMV internal users and external users. 9. DMV restricts network services that traverse LAN and WAN networking segments. 10. Direct remote access to any computer is not allowed. 11. Standalone modems are not allowed 12. Vendor provided remote control applications are not allowed. 13. Servers and User PC’s are restricted from residing on the same network segment. 14. Any proposed system or optional configuration must have an automatic restart process for connection failures or if the back end systems are unavailable. 15. System must provide future growth estimates and hardware requirements to support future growth and scalability. 16. Any customer record information that is accessed must be encrypted via known industry security methodologies and be fully documented.	
	Supplemental Guidance: Information systems are capable of providing a wide variety of functions and services. Some of the functions and services, provided by default, may not be necessary to support essential organizational operations (e.g., key missions, functions). Additionally, it is sometimes convenient to provide multiple services from a single component of an information system, but doing so increases risk over limiting the services provided by any one component.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Where feasible, organizations limit component functionality to a single function per device (e.g., email server or web server, not both). The functions and services provided by organizational information systems, or individual components of information systems, are carefully reviewed to determine which functions and services are candidates for elimination (e.g., Voice Over Internet Protocol, Instant Messaging, auto-execute, file sharing). Organizations consider disabling unused or unnecessary physical and logical ports and protocols (e.g., Universal Serial Bus [USB], File Transfer Protocol [FTP], Internet Protocol Version 6 [IPv6], Hyper Text Transfer Protocol [HTTP]) on information system components to prevent unauthorized connection of devices, unauthorized transfer of information, or unauthorized tunneling. Organizations can utilize network scanning tools, intrusion detection and prevention systems, and end-point protections such as firewalls and host-based intrusion detection systems to identify and prevent the use of prohibited functions, ports, protocols, and services. Related control: RA-5.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization reviews the information system once a year at a minimum to identify and eliminate unnecessary functions, ports, protocols, and/or services.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. 2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) 2.2.2 Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	
CM-8	**INFORMATION SYSTEM COMPONENT INVENTORY**	Previous SEC 501-06 Control References: 10.2.3
	Control: The organization develops, documents, and maintains an inventory of information system components that:	
a.	Accurately reflects the current information system;	
b.	Is consistent with the authorization boundary of the information system;	
c.	Is at the level of granularity deemed necessary for tracking and reporting;	
d.	Includes using the System Inventory and Definition Template in order to achieve effective property accountability **(Please see *FORMS* section of this document).**	
e.	Is available for review and audit by designated organizational officials.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Information deemed to be necessary by the organization to achieve effective property accountability can include, for example, hardware inventory specifications (manufacturer, type, model, serial number, physical location), software license information, information system/component owner, and for a networked component/device, the machine name and network address. Related controls: CM-2, CM-6.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates.	
(4)	The organization includes in property accountability information for information system components, a means for identifying by name, position and role, individuals responsible for administering those components.	
(5)	The organization verifies that all components within the authorization boundary of the information system are either inventoried as a part of the system or recognized by another system as a component within that system.	
(6)	The organization includes assessed component configurations and any approved deviations to current deployed configurations in the information system component inventory.	
	Enhancement Supplemental Guidance: This control enhancement focuses on the configuration settings established by the organization for its information system components, the specific information system components that have been assessed to determine compliance with the required configuration settings, and any approved deviations from established configuration settings in the deployed information system components. Related controls: CM-2, CM-6.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: Purpose Sensitive IT System Inventory and Definition requirements identify the steps in listing and marking the boundaries of sensitive IT systems in order to provide cost-effective, risk-based security protection for IT systems, for the agency as a whole, and for the COV enterprise. 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. **Notes:** - Data and homogenous systems, belonging to a single agency, that have the same technical controls and account management procedures (i.e., Microsoft SharePoint, or PeopleSoft), may be classified and grouped as a single set of data or systems for the purpose of inventory, data classification, risk assessments, security audits, etc. - Where more than one agency may own the IT system, and the agency or agencies cannot reach consensus on which should serve as System Owner for the purposes of this Standard, upon request, the CIO of the Commonwealth will determine the System Owner. - A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a single System Owner. 2. Maintain or require that its service provider maintain updated network diagrams. Please refer to the current version of VITA's ***ITRM SEC506 Risk Assessment Guideline*** , section 5 for additional instructions. VITA CM-8	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: And the Device list aspect of: 12.3.3 A list of all such devices and personnel with access.	
CM-9	**CONFIGURATION MANAGEMENT PLAN**	Previous SEC 501-06 Control References: 10.4
	Control: The organization develops, documents, and implements a configuration management plan for the information system that:	
a.	Addresses roles, responsibilities, and configuration management processes and procedures;	
b.	Defines the configuration items for the information system and when in the system development life cycle the configuration items are placed under configuration management; and	
c.	Establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Configuration items are the information system items (hardware, software, firmware, and documentation) to be configuration managed. The configuration management plan satisfies the requirements in the organization's configuration management policy while being tailored to the individual information system. The configuration management plan defines detailed processes and procedures for how configuration management is used to support system development life cycle activities at the information system level. The plan describes how to move a change through the change management process, how configuration settings and configuration baselines are updated, how the information system component inventory is maintained, how development, test, and operational environments are controlled, and finally, how documents are developed, released, and updated. The configuration management approval process includes designation of key management stakeholders that are responsible for reviewing and approving proposed changes to the information system, and security personnel that would conduct an impact analysis prior to the implementation of any changes to the system. Related control: SA-10.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization assigns responsibility for developing the configuration management process to organizational personnel that are not directly involved in system development.	
	Enhancement Supplemental Guidance: In the absence of a dedicated configuration management team, the system integrator may be tasked with developing the configuration management process.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations 6.4.5 Change control procedures for the implementation of security patches and software modifications.	
2.6	***FAMILY:*** *CONTINGENCY PLANNING*	***CLASS:*** *OPERATIONAL*
CP-2	**CONTINGENCY PLAN**	Previous SEC 501-06 Control References: 3.1
	Control: The organization:	
a.	Develops a contingency plan for the information system that:	
	Identifies essential missions and business functions and associated contingency requirements;	
	Provides recovery objectives, restoration priorities, and metrics;	
	Addresses contingency roles, responsibilities, assigned individuals with contact information;	
	Addresses maintaining essential missions and business functions despite an information system disruption, compromise, or failure;	
	Addresses eventual, full information system restoration without deterioration of the security measures originally planned and implemented; and	
	Is reviewed and approved by designated officials within the organization;	
b.	Distributes copies of the contingency plan to all Administrations and key personnel within the agency, and to others as deemed appropriate;	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
c.	Coordinates contingency planning activities with incident handling activities;	
d.	Reviews the contingency plan for the information system once a year at a minimum;	
e.	Revises the contingency plan to address changes to the organization, information system, or environment of operation and problems encountered during contingency plan implementation, execution, or testing; and	
f.	Communicates contingency plan changes to all Administrations and key personnel within the agency, and others as deemed appropriate.	
	Supplemental Guidance: Contingency planning for information systems is part of an overall organizational program for achieving continuity of operations for mission/business operations. Contingency planning addresses both information system restoration and implementation of alternative mission/business processes when systems are compromised. Information system recovery objectives are consistent with applicable laws, directives, policies, standards, or regulations. In addition to information system availability, contingency plans also address other security-related events resulting in a reduction in mission/business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system. Examples of actions to call out in contingency plans include, for example, graceful degradation, information system shutdown, fall back to a manual mode, alternate information flows, or operating in a mode that is reserved solely for when the system is under attack. Related controls: AC-14, CP-6, CP-7, CP-8, IR-4, PM-8, PM-11.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization coordinates contingency plan development with organizational elements responsible for related plans.	
	Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	
(2)	The organization conducts capacity planning so that necessary capacity for information processing, telecommunications, and environmental support exists during contingency operations.	
(3)	The organization plans for the resumption of essential missions and business functions within 24 hours of contingency plan activation.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Business recovery and continuity procedures § Data back-up processes	
CP-3	**CONTINGENCY TRAINING**	Previous SEC 501-06 Control References: 3.2.2.3
	Control: The organization trains personnel in their contingency roles and responsibilities with respect to the information system and provides refresher training once a year at a minimum or within 30-days of a role or assignment change.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(1)	The organization incorporates simulated events into contingency training to facilitate effective response by personnel in crisis situations.	
	PCI compliance: PCI-DSS has no requirement for this control.	
CP-4	**CONTINGENCY PLAN TESTING AND EXERCISES**	Previous SEC 501-06 Control References: 3.2.2.4
	Control: The organization:	
a.	Tests and/or exercises the contingency plan for the information system once a year at a minimum or when the contingency plan is revised to determine the plan's effectiveness and the organization's readiness to execute the plan; and	
b.	Reviews the contingency plan test/exercise results and initiates corrective actions.	
	Supplemental Guidance: There are several methods for testing and/or exercising contingency plans to identify potential weaknesses (e.g., checklist, walk-through/tabletop, simulation: parallel, full interrupt). Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets (e.g., reduction in mission capability) and individuals arising due to contingency operations in accordance with the plan.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization coordinates contingency plan testing and/or exercises with organizational elements responsible for related plans.	
	Enhancement Supplemental Guidance: Examples of related plans include Business Continuity Plan, Disaster Recovery Plan, Continuity of Operations Plan, Crisis Communications Plan, Critical Infrastructure Plan, Cyber Incident Response Plan, and Occupant Emergency Plan.	
(2)	The organization tests/exercises the contingency plan at the alternate processing site to familiarize contingency personnel with the facility and available resources and to evaluate the site's capabilities to support contingency operations.	
(4)	The organization includes a full recovery and reconstitution of the information system to a known state as part of contingency plan testing.	
	Enhancement Supplemental Guidance: Related controls: CP-10, SC-24.	
	PCI compliance: PCI-DSS has no requirement for this control.	
CP-6	**ALTERNATE STORAGE SITE**	Previous SEC 501-06 Control References: 3.4.2.1
	Control: The organization establishes an alternate storage site including necessary agreements to permit the storage and recovery of information system backup information.	
	Supplemental Guidance: Related controls: CP-2, CP-9, MP-4.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization identifies an alternate storage site that is separated from the primary storage site so as not to be susceptible to the same hazards.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: Hazards of concern to the organization are typically defined in an organizational assessment of risk.	
(2)	The organization configures the alternate storage site to facilitate recovery operations in accordance with recovery time and recovery point objectives.	
(3)	The organization identifies potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
	Enhancement Supplemental Guidance: Explicit mitigation actions include, for example, duplicating backup information at another alternate storage site if access to the first alternate site is hindered; or, if electronic accessibility to the alternate site is disrupted, planning for physical access to retrieve backup information.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually. 9.6 Physically secure all media. 9.9 Maintain strict control over the storage and accessibility of media. 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers. 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	
CP-7	**ALTERNATE PROCESSING SITE**	Previous SEC 501-06 Control References: None
	Control: The organization:	
a.	Establishes an alternate processing site including necessary agreements to permit the resumption of information system operations for essential missions and business functions; and	
b.	Ensures that equipment and supplies required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption.	
	Supplemental Guidance: Related control: CP-2.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization identifies an alternate processing site that is separated from the primary processing site so as not to be susceptible to the same hazards.	
	Enhancement Supplemental Guidance: Hazards that might affect the information system are typically defined in the risk assessment.	
(2)	The organization identifies potential accessibility problems to the alternate processing site in the event of an area-wide disruption or disaster and outlines explicit mitigation actions.	
(3)	The organization develops alternate processing site agreements that contain priority-of-service provisions in accordance with the organization's availability requirements.	
(4)	The organization configures the alternate processing site so that it is ready to be used as the operational site supporting essential missions and business functions.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(5)	The organization ensures that the alternate processing site provides information security measures equivalent to that of the primary site.	
	PCI compliance: PCI-DSS has no requirement for this control.	
CP-8	**TELECOMMUNICATIONS SERVICES**	Previous SEC 501-06 Control References: 3.1
	Control: The organization establishes alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential missions and business functions within the organization-defined time period when the primary telecommunications capabilities are unavailable.	
	Supplemental Guidance: Related control: CP-2.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization:	
(a)	Develops primary and alternate telecommunications service agreements that contain priority of- service provisions in accordance with the organization's availability requirements; and	
(b)	Requests Telecommunications Service Priority for all telecommunications services used for emergency preparedness in the event that the primary and/or alternate telecommunications services are provided by a common carrier.	
(2)	The organization obtains alternate telecommunications services with consideration for reducing the likelihood of sharing a single point of failure with primary telecommunications services.	
(3)	The organization obtains alternate telecommunications service providers that are separated from primary service providers so as not to be susceptible to the same hazards.	
(4)	The organization requires primary and alternate telecommunications service providers to have contingency plans.	
	PCI compliance: PCI-DSS has no requirement for this control.	
CP-9	**INFORMATION SYSTEM BACKUP**	Previous SEC 501-06 Control References: 3.4.2.9
	Control: The organization:	
a.	Conducts backups of user-level information contained in the information system;	
b.	Conducts backups of system-level information contained in the information system;	
c.	Conducts backups of information system documentation including security-related documentation; and	
d.	Protects the confidentiality and integrity of backup information at the storage location.	
	Supplemental Guidance: System-level information includes, for example, system-state information, operating system and application software, and licenses. Digital signatures and cryptographic hashes are examples of mechanisms that can be employed by organizations to protect the integrity of information system backups. An organizational assessment of risk guides the use of encryption for protecting backup information. The protection of system backup information while in transit is beyond the scope of this control. Related controls: CP-6, MP-4.	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(1)	The organization tests backup information every 30-days at a minimum to verify media reliability and information integrity.	
(2)	The organization uses a sample of backup information in the restoration of selected information system functions as part of contingency plan testing.	
(3)	The organization stores backup copies of the operating system and other critical information system software, as well as copies of the information system inventory (including hardware, software, and firmware components) in a separate facility or in a fire-rated container that is not collocated with the operational system.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Data back-up processes	
CP-10	**INFORMATION SYSTEM RECOVERY AND RECONSTITUTION**	Previous SEC 501-06 Control References: 3.4
	Control: The organization provides for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure.	
	Supplemental Guidance: Recovery is executing information system contingency plan activities to restore essential missions and business functions. Reconstitution takes place following recovery and includes activities for returning the information system to its original functional state before contingency plan activation. Recovery and reconstitution procedures are based on organizational priorities, established recovery point/time and reconstitution objectives, and appropriate metrics. Reconstitution includes the deactivation of any interim information system capability that may have been needed during recovery operations. Reconstitution also includes an assessment of the fully restored information system capability, a potential system reauthorization and the necessary activities to prepare the system against another disruption, compromise, or failure. Recovery and reconstitution capabilities employed by the organization can be a combination of automated mechanisms and manual procedures. Related controls: CA-2, CA-6, CA-7, SC-24.	
	Control Enhancements for Sensitive Systems:	
(2)	The information system implements transaction recovery for systems that are transaction-based.	
	Enhancement Supplemental Guidance: Database management systems and transaction processing systems are examples of information systems that are transaction-based. Transaction rollback and transaction journaling are examples of mechanisms supporting transaction recovery.	
(3)	The organization provides compensating security controls for those organization-defined circumstances that can inhibit recovery and reconstitution to a known state.	
(4)	The organization provides the capability to reimage information system components within the organization-defined restoration time-periods from configuration-controlled and integrity-protected disk images representing a secure, operational state for the components.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Business recovery and continuity procedures	
2.7	***FAMILY:*** *IDENTIFICATION AND AUTHENTICATION*	***CLASS:*** *TECHNICAL*
IA-2	**IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**	Previous SEC 501-06 Control References: 5.3.2.5
	Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).	
	Supplemental Guidance: Organizational users include organizational employees or individuals the organization deems to have equivalent status of employees (e.g., contractors, guest researchers, individuals from allied nations). Users are uniquely identified and authenticated for all accesses other than those accesses explicitly identified and documented by the organization in AC-14. Unique identification of individuals in group accounts (e.g., shared privilege accounts) may need to be considered for detailed accountability of activity. Authentication of user identities is accomplished through the use of passwords, tokens, biometrics, or in the case of multifactor authentication, some combination thereof. Access to organizational information systems is defined as either local or network. Local access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained by direct connection without the use of a network. Network access is any access to an organizational information system by a user (or process acting on behalf of a user) where such access is obtained through a network connection. Remote access is a type of network access which involves communication through an external network (e.g., the Internet). Internal networks include local area networks, wide area networks, and virtual private networks that are under the control of the organization. For a virtual private network (VPN), the VPN is considered an internal network if the organization establishes the VPN connection between organization-controlled endpoints in a manner that does not require the organization to depend on any external networks across which the VPN transits to protect the confidentiality and integrity of information transmitted. Identification and authentication requirements for information system access by other than organizational users are described in IA-8. Related controls: AC-14, AC-17, AC-18, IA-4, IA-5.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.1 Assign all users a unique username before allowing them to access system components or cardholder data. 8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: § Something you know, such as a password or passphrase § Something you have, such as a token device or smart card § Something you are, such as a biometric	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
IA-4	**IDENTIFIER MANAGEMENT**	Previous SEC 501-06 Control References: 5.4.2.4
	Control: The organization manages information system identifiers for users and devices by:	
a.	Receiving authorization from a designated organizational official to assign a user or device identifier;	
b.	Selecting an identifier that uniquely identifies an individual or device;	
c.	Assigning the user identifier to the intended party or the device identifier to the intended device;	
d.	Preventing reuse of user or device identifiers for a period of one-year at a minimum; and	
e.	Disabling the user identifier after 90-days of inactivity.	
	Supplemental Guidance: Common device identifiers include media access control (MAC) or Internet protocol (IP) addresses, or device-unique token identifiers. Management of user identifiers is not applicable to shared information system accounts (e.g., guest and anonymous accounts). It is commonly the case that a user identifier is the name of an information system account associated with an individual. In such instances, identifier management is largely addressed by the account management activities of AC-2. IA-4 also covers user identifiers not necessarily associated with an information system account (e.g., the identifier used in a physical security control database accessed by a badge reader system for access to the information system). Related control: AC-2, IA-2.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.1 Assign all users a unique username before allowing them to access system components or cardholder data. 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: 8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. 8.5.5 Remove/disable inactive user accounts at least every 90 days.	
IA-5	**AUTHENTICATOR MANAGEMENT**	Previous SEC 501-06 Control References: 5.3
	Control: The organization manages information system authenticators for users and devices by:	
a.	Verifying, as part of the initial authenticator distribution, the identity of the individual and/or device receiving the authenticator;	
b.	Establishing initial authenticator content for authenticators defined by the organization;	
c.	Ensuring that authenticators have sufficient strength of mechanism for their intended use;	
d.	Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators;	
e.	Changing default content of authenticators upon information system installation;	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
f.	Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators (if appropriate);	
g.	Changing/refreshing authenticators every 90-days at a minimum;	
h.	Protecting authenticator content from unauthorized disclosure and modification; and	
i.	Requiring users to take, and having devices implement, specific measures to safeguard authenticators.	
	Supplemental Guidance: User authenticators include, for example, passwords, tokens, biometrics, PKI certificates, and key cards. Initial authenticator content is the actual content (e.g., the initial password) as opposed to requirements about authenticator content (e.g., minimum password length). Many information system components are shipped with factory default authentication credentials to allow for initial installation and configuration. Default authentication credentials are often well known, easily discoverable, present a significant security risk, and therefore, are changed upon installation. The requirement to protect user authenticators may be implemented via control PL-4 or PS-6 for authenticators in the possession of users and by controls AC-3, AC-6, and SC-28 for authenticators stored within the information system (e.g., passwords stored in a hashed or encrypted format, files containing encrypted or hashed passwords accessible only with super user privileges). The information system supports user authenticator management by organization-defined settings and restrictions for various authenticator characteristics including, for example, minimum password length, password composition, validation time window for time synchronous one time tokens, and number of allowed rejections during verification stage of biometric authentication. Measures to safeguard user authenticators include, for example, maintaining possession of individual authenticators, not loaning or sharing authenticators with others, and reporting lost or compromised authenticators immediately. Authenticator management includes issuing and revoking, when no longer needed, authenticators for temporary access such as that required for remote maintenance. Device authenticators include, for example, certificates and passwords. Related controls: AC-2, IA-2, PL-4, PS-6.	
	Control Enhancements for Sensitive Systems:	
(1)	The information system, for password-based authentication:	
(a)	Enforces minimum password complexity of:	
a.	At least eight characters in length; and	
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;	
(c)	Encrypts passwords in storage and in transmission;	
(d)	Enforces password minimum and maximum lifetime restrictions of 24 hours minimum and 90 days maximum; and	
(e)	Prohibits password reuse for 24 generations.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: This control enhancement is intended primarily for environments where passwords are used as a single factor to authenticate users, or in a similar manner along with one or more additional authenticators. The enhancement generally does not apply to situations where passwords are used to unlock hardware authenticators. The implementation of such password mechanisms may not meet all of the requirements in the enhancement.	
(5)	The organization requires vendors and/or manufacturers of information system components to provide unique authenticators or change default authenticators prior to delivery.	
	Enhancement Supplemental Guidance: This control enhancement extends the requirement for organizations to change default authenticators upon information system installation.	
(6)	The organization protects authenticators commensurate with the classification or sensitivity of the information accessed.	
(7)	The organization ensures that unencrypted static authenticators are not embedded in applications or access scripts or stored on function keys.	
	Enhancement Supplemental Guidance: Organizations exercise caution in determining whether an embedded or stored authenticator is in encrypted or unencrypted form. If the authenticator in its stored representation, is used in the manner stored, then that representation is considered an unencrypted authenticator. This is irrespective of whether that representation is perhaps an encrypted version of something else (e.g., a password).	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: Render all passwords unreadable during transmission and storage on all system components using strong cryptography. PCI 8.4 VITA IA-5 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use. PCI 8.5.3 VITA IA-5 Immediately revoke access for any terminated users. PCI 8.5.4 VITA IA-5 Configure sensitive IT systems to allow users to change their password at will. Require users of sensitive IT systems to include network systems to change their passwords at least every 90 days. PCI 8.5.9 VITA IA-5 At least nine characters in length PCI 8.5.10 VITA IA-5	
	Utilize at least three of the following four: i. Lowercase alpha (e.g. abc) ii. Uppercase alpha (e.g. ABC) iii. Numeric (e.g. 123) iv. Special/Non-Alphanumeric characters (e.g. ! $ # %) PCI 8.5.11 VITA IA-5 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 PCI 8.5.11 VITA IA-5	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 2.1 Always change vendor-supplied defaults before installing a system on the network—including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts. 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography. 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: 8.5.2 Verify user identity before performing password resets. 8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use. 8.5.4 Immediately revoke access for any terminated users. 8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods. 8.5.9 Change user passwords at least every 90 days. 8.5.10 Require a minimum password length of at least seven characters. 8.5.11 Use passwords containing both numeric and alphabetic characters. 8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	
IA-6	**AUTHENTICATOR FEEDBACK**	Previous SEC 501-06 Control References: 5.3.2.17
	Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.	
	Supplemental Guidance: The feedback from the information system does not provide information that would allow an unauthorized user to compromise the authentication mechanism. Displaying asterisks when a user types in a password, is an example of obscuring feedback of authentication information.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
IA-7	**CRYPTOGRAPHIC MODULE AUTHENTICATION**	Previous SEC 501-06 Control References: None
	Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for such authentication.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.5.3 Insecure cryptographic storage.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
IA-8	**IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS)**	Previous SEC 501-06 Control References: None
	Control: The information system uniquely identifies and authenticates non-organizational users (or processes acting on behalf of non-organizational users).	
	Supplemental Guidance: None. Related controls: AC-14, AC-17, AC-18, MA-4.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS requirements make no distinction between organizational vs. non-organizational users; all must be uniquely identified and authenticated.	
2.8	***FAMILY:*** *INCIDENT RESPONSE*	***CLASS:*** *OPERATIONAL*
IR-1-COV	**INCIDENT RESPONSE (COV)**	Previous SEC 501-06 Control References: 9.2.2/9.3.2/9.4.2
	Control: 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.	
2	Implement Intrusion Detection System (IDS) and Intrusion Prevention System (IPS).	
3	Conduct IDS and IPS log reviews to detect new attack patterns as quickly as possible.	
4	Develop and implement required mitigation measures based on the results of IDS and IPS log reviews.	
5	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:	
a.	Designate individuals responsible for the development and implementation of information security logging capabilities, as well as detailed procedures for reviewing and administering the logs.	
b.	Document standards that specify the type of actions an IT system should take when a suspicious or apparent malicious activity is taking place.	
c.	Prohibit the installation or use of unauthorized monitoring devices.	
d.	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.	
6	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:	
a.	Designate an Information Security Incident Response Team that includes personnel with appropriate expertise for responding to cyber attacks.	
b.	Identify controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
c.	Implement proactive measures based on cyber attacks to defend against new forms of cyber attacks and zero-day exploits.	
d.	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.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date. 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	
IR-2	**INCIDENT RESPONSE TRAINING**	Previous SEC 501-06 Control References: 8.3.2.3
	Control: The organization:	
a.	Trains personnel in their incident response roles and responsibilities with respect to the information system; and	
b.	Provides refresher training once a year at a minimum or whenever the Incident Response procedures are modified.	
	Supplemental Guidance: Incident response training includes user training in the identification and reporting of suspicious activities, both from external and internal sources. Related control: AT-3.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization incorporates simulated events into incident response training to facilitate effective response by personnel in crisis situations.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.4 Provide appropriate training to staff with security breach response responsibilities.	
IR-3	**INCIDENT RESPONSE TESTING AND EXERCISES**	Previous SEC 501-06 Control References: None
	Control: The organization tests and/or exercises the incident response capability for the information system once a year at a minimum using the existing incident response procedures to determine the incident response effectiveness and documents the results.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.2 Test the plan at least annually.	
IR-4	**INCIDENT HANDLING**	Previous SEC 501-06 Control References: 9.4.2
	Control: The organization:	
a.	Implements an incident handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery;	
b.	Coordinates incident handling activities with contingency planning activities; and	
c.	Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing/exercises, and implements the resulting changes accordingly.	
	Supplemental Guidance: Incident-related information can be obtained from a variety of sources including, but not limited to, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports. Related controls: AU-6, CP-2, IR-2, IR-3, PE-6, SC-5, SC-7, SI-3, SI-4, SI-7.	
	Control Enhancements for Sensitive Systems:	
(3)	The organization identifies classes of incidents and defines appropriate actions to take in response to ensure continuation of organizational missions and business functions.	
	Enhancement Supplemental Guidance: Classes of incidents include, for example, malfunctions due to design/implementation errors and omissions, targeted malicious attacks, and untargeted malicious attacks. Incident response actions that may be appropriate include, for example, graceful degradation, information system shutdown, fall back to manual mode or alternative technology whereby the system operates differently, employing deceptive measures (e.g., false data flows, false status measures), alternate information flows, or operating in a mode that is reserved solely for when a system is under attack.	
(4)	The organization correlates incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	
IR-4-COV	**INCIDENT HANDLING (COV)**	Previous SEC 501-06 Control References: 9.4.2

No.	Control Family / Control Name / Guidance	Control Class / Prior References
1	**Control: 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.**	
2	Establish procedures for information security incident investigation, preservation of evidence, and forensic analysis.	
	DMV-Specific Requirements: The IT Security Director shall or shall require that its service provider (VITA) ensure that the following requirements are met in the collection of evidence: 1. To provide evidence for investigation, prosecution, and disciplinary actions, certain information must be immediately captured whenever a computer crime or abuse is suspected. a. The information to be immediately collected includes the current system configuration as well as copies of all potentially involved files. b. The information acquired must then be securely stored off-line until official custody is given to another authorized person. 2. For every production computer system, DMV ISO must identify the sources of digital evidence that could reasonably be used in a court case. a. These sources of evidence must then be subject to a standardized capture, retention, and destruction process comparable to that used for vital records. 3. All analysis or investigation must be performed with a copy rather than the original storage media. This prevents unexpected modification of the original information. 4. All DMV internal investigations of actual or potential information security incidents or violations, must be conducted by trained staff authorized by the IT Security Director or Law Enforcement Services (LES). 5. Until charges are pressed or disciplinary action taken, all investigations of alleged criminal or abusive conduct must be kept strictly confidential to preserve the reputation of the suspect. 6. To prevent conflict of interest, anyone having a personal relationship with the suspect is barred from participating in the incident investigation. 7. Please refer to DMV's *Incident Response Plan* , appendix **Media Forensics** for procedure on forensic acquisition and e-Discovery. PCI 12.9 IR-4-COV	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
IR-4-COV-2	**INCIDENT HANDLING (COV-2)**	Previous SEC 501-06 Control References: 9.5.2
	Control: 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:	
1	Identify and document all agency systems, processes, and logical or physical data storage locations (whether held by the agency or a third party) that contain personal information or medical information.	
a.	Personal information 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 that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:	
i.	Social security number;	
ii.	Drivers license number or state identification card number issued in lieu of a driver's license number; or	
iii.	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;	
b.	Medical information 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 that relate to a resident of the Commonwealth, when the data elements are neither encrypted nor redacted:	
i.	Any information regarding an individual's medical or mental health history, mental or physical condition, or medical treatment or diagnosis by a health care professional; or	
ii.	An individual's health insurance policy number or subscriber identification number, any unique identifier used by a health insurer to identify the individual, or any information in an individual's application and claims history, including any appeals records.	
2	"Redact" for personal information means alteration or truncation of data such that no more than the following are accessible as part of the personal 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.	
3	"Redact" for medical information means alteration or truncation of data such that no information regarding the following are accessible as part of the medical information:	
a.	An individual's medical history; or	
b.	Mental or physical condition; or	
c.	Medical treatment or diagnosis; or	
d.	No more than four digits of a health insurance policy number, subscriber number; or	
e.	Other unique identifier.	
4	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	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
b.	Allow the agency to both participate in the investigation of incidents and exercise control over decisions regarding external reporting.	
5	Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted personal information or medical 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; and	
c.	Security compromise of any system containing personal or medical information (i.e., social security numbers, credit card numbers, medical records, insurance policy numbers, laboratory findings, pharmaceutical regimens, medical or mental diagnosis, medical claims history, medical appeals records, etc.).	
6	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.	
7	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.	
8	The agency shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #9, below.	
9	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.	
10	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 (i.e., credit report, medical insurance Explanation of Benefits (EOB), etc.).	
11	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	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
iii.	Notice to major statewide media. 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 longer impede the investigation or jeopardize national or homeland security.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	
IR-5	**INCIDENT MONITORING**	Previous SEC 501-06 Control References: 9.4.2
	Control: The organization tracks and documents information system security incidents.	
	Supplemental Guidance: Documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics, evaluating incident details, trends, and handling. Incident information can be obtained from a variety of sources including, for example, incident reports, incident response teams, audit monitoring, network monitoring, physical access monitoring, and user/administrator reports.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	
IR-5-COV	**INCIDENT MONITORING (COV)**	Previous SEC 501-06 Control References: 9.3.2.3
	Control: Routinely monitor IT system event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	
IR-6	**INCIDENT REPORTING**	Previous SEC 501-06 Control References: 9.4.2
	Control: The organization:	
a.	Requires personnel to report suspected security incidents to the organizational incident response capability within 24 hours from when the department discovered or should have discovered their occurrence; and	
b.	Reports security incident information to designated authorities.	
	Supplemental Guidance: The intent of this control is to address both specific incident reporting requirements within an organization and the formal incident reporting requirements for Commonwealth agencies. The types of security incidents reported, the content and timeliness of the reports, and the list of designated reporting authorities are consistent with applicable laws, directives, policies, regulations, standards, and guidance. Related controls: IR-4, IR-5.	
	Control Enhancements for Sensitive Systems:	
(2)	The organization reports information system weaknesses, deficiencies, and/or vulnerabilities associated with reported security incidents to appropriate organizational officials.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum § Analysis of legal requirements for reporting compromises § Reference or inclusion of incident response procedures from the payment brands	
IR-6-COV	**INCIDENT REPORTING (COV)**	Previous SEC 501-06 Control References: 9.2.2.6/9.4.2.6
1	**Control: Provide quarterly summary reports of IDS and IPS events to Commonwealth Security.**	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
2	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."	
3	Report information security incidents only through channels that have not been compromised.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Analysis of legal requirements for reporting compromises	
IR-7	**INCIDENT RESPONSE ASSISTANCE**	Previous SEC 501-06 Control References: 9.4.2
	Control: The organization provides an incident response support resource, integral to the organizational incident response capability, that offers advice and assistance to users of the information system for the handling and reporting of security incidents.	
	Supplemental Guidance: Possible implementations of incident response support resources in an organization include a help desk or an assistance group and access to forensics services, when required. Related controls: IR-4, IR-6.	
	Control Enhancements for Sensitive Systems:	
(2)	The organization:	
(a)	Establishes a direct, cooperative relationship between its incident response capability and external providers of information system protection capability; and	
(b)	Identifies organizational incident response team members to the external providers.	
	Enhancement Supplemental Guidance: External providers of information system protection capability include, for example, the Computer Network Defense program within the U.S. Department of Defense. External providers help to protect, monitor, analyze, detect, and respond to unauthorized activity within organizational information systems and networks.	
	PCI compliance: PCI-DSS has no requirement for this control.	
IR-8	**INCIDENT RESPONSE PLAN**	Previous SEC 501-06 Control References: 9.4.2

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control: The organization:	
a.	Develops an incident response plan that:	
	Provides the organization with a roadmap for implementing its incident response capability;	
	Describes the structure and organization of the incident response capability;	
	Provides a high-level approach for how the incident response capability fits into the overall organization;	
	Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;	
	Defines reportable incidents;	
	Provides metrics for measuring the incident response capability within the organization.	
	Defines the resources and management support needed to effectively maintain and mature an incident response capability; and	
	Is reviewed and approved by designated officials within the organization;	
b.	Distributes copies of the incident response plan to the Incident Response Team and Management, and to others as deemed appropriate.	
c.	Reviews the incident response plan once a year at a minimum;	
d.	Revises the incident response plan to address system/organizational changes or problems encountered during plan implementation, execution, or testing; and	
e.	Communicates incident response plan changes to the Incident Response Team and Management, and to others as deemed appropriate.	
	Supplemental Guidance: It is important that organizations have a formal, focused, and coordinated approach to responding to incidents. The organization's mission, strategies, and goals for incident response help determine the structure of its incident response capability.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach. 12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	
2.9	***FAMILY:*** *MAINTENANCE*	***CLASS:*** *OPERATIONAL*
MA-2	**CONTROLLED MAINTENANCE**	Previous SEC 501-06 Control References: None
	Control: The organization:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Schedules, performs, documents, and reviews records of maintenance and repairs on information system components in accordance with manufacturer or vendor specifications and/or organizational requirements;	
b.	Controls all maintenance activities, whether performed on site or remotely and whether the equipment is serviced on site or removed to another location;	
c.	Requires that a designated official explicitly approve the removal of the information system or system components from organizational facilities for off-site maintenance or repairs;	
d.	Sanitizes equipment to remove all information from associated media prior to removal from organizational facilities for off-site maintenance or repairs; and	
e.	Checks all potentially impacted security controls to verify that the controls are still functioning properly following maintenance or repair actions.	
	Supplemental Guidance: The control is intended to address the information security aspects of the organization's information system maintenance program. Related controls: MP-6, SI-2.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
MA-5	**MAINTENANCE PERSONNEL**	Previous SEC 501-06 Control References: None
	Control: The organization:	
a.	Establishes a process for maintenance personnel authorization and maintains a current list of authorized maintenance organizations or personnel; and	
b.	Ensures that personnel performing maintenance on the information system have required access authorizations or designates organizational personnel with required access authorizations and technical competence deemed necessary to supervise information system maintenance when maintenance personnel do not possess the required access authorizations.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Individuals not previously identified in the information system, such as vendor personnel and consultants, may legitimately require privileged access to the system, for example, when required to conduct maintenance or diagnostic activities with little or no notice. Based on a prior assessment of risk, the organization may issue temporary credentials to these individuals. Temporary credentials may be for one-time use or for a very limited time period. Related controls: IA-8, MA-5.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8.1 Maintain a list of service providers.	
2.10	***FAMILY:*** *MEDIA PROTECTION*	***CLASS:*** *OPERATIONAL*
MP-2	**MEDIA ACCESS**	Previous SEC 501-06 Control References: 6.2.2.4
	Control: The organization restricts access to digital and non-digital media to only authorized individuals using appropriate security measures.	
	Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, external/removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices). An organizational assessment of risk guides the selection of media and associated information contained on that media requiring restricted access. Organizations document in policy and procedures, the media requiring restricted access, individuals authorized to access the media, and the specific measures taken to restrict access. Fewer protection measures are needed for media containing information determined by the organization to be in the public domain, to be publicly releasable, or to have limited or no adverse impact if accessed by other than authorized personnel. In these situations, it is assumed that the physical access controls where the media resides provide adequate protection. Related controls: MP-4, PE-3.	
	Control Enhancements for Sensitive Systems:	
	Enhancement Supplemental Guidance: This control enhancement is primarily applicable to media storage areas within an organization where a significant volume of media is stored and is not applicable to every location where some media is stored (e.g., in individual offices).	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.6 Physically secure all media. 9.7 Maintain strict control over the internal or external distribution of any kind of media. 9.9 Maintain strict control over the storage and accessibility of media.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
MP-3	**MEDIA MARKING**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization:	
a.	Marks, in accordance with organizational policies and procedures, removable information system media and information system output indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.7.1 Classify media so the sensitivity of the data can be determined.	
MP-4	**MEDIA STORAGE**	Previous SEC 501-06 Control References: 6.2.2.4
	Control: The organization:	
a.	Physically controls and securely stores digital and non-digital media.	
b.	Protects information system media until the media are destroyed or sanitized using approved equipment, techniques, and procedures.	
	Supplemental Guidance: The strength of mechanisms is commensurate with the classification and sensitivity of the information. Related controls: AC- 3, AC-19, CP-6, CP-9, MP-2, PE-3.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs cryptographic mechanisms to protect information in storage.	
	Enhancement Supplemental Guidance: Requires documented approval from the agency head. Related control: SC-13.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: The following restrictions apply to all work areas at DMV. The IT Security Director shall or shall require its service provider (VITA) ensure that the following requirements are met for protecting COV data: 1. DMV employees, contractors, consultants and vendors shall observe a clean desk policy: all sensitive or confidential information, regardless of media, shall be properly secured at all times unless being actively worked on. 2. Proper storage of digital or non-digital media that contains sensitive or confidential information requires that it be secured in a locked file cabinet, desk, safe, or other heavy furniture. 3. Sensitive or confidential information shall not be left unattended in unsecured areas; i.e., left in a conference room during breaks or overnight. PCI 9.6, 9.9 VITA MP-4	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually. 9.6 Physically secure all media. 9.9 Maintain strict control over the storage and accessibility of media.	
MP-5	**MEDIA TRANSPORT**	Previous SEC 501-06 Control References: 6.2.2.4
	Control: The organization:	
a.	Protects and controls digital and non-digital media during transport outside of controlled areas.	
b.	Maintains accountability for information system media during transport outside of controlled areas; and	
c.	Restricts the activities associated with transport of such media to authorized personnel.	
	Supplemental Guidance: Information system media includes both digital media (e.g., diskettes, magnetic tapes, removable hard drives, flash/thumb drives, compact disks, digital video disks) and non-digital media (e.g., paper, microfilm). This control also applies to mobile computing and communications devices with information storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones, digital cameras, and audio recording devices) that are transported outside of controlled areas. Locked containers and cryptography are examples of security measures available to protect digital and non-digital media during transport. Cryptographic mechanisms can provide confidentiality and/or integrity protections depending upon the mechanisms used. Related controls: AC-19, CP-9.	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(2)	The organization documents activities associated with the transport of information system media.	
	Enhancement Supplemental Guidance: Organizations establish documentation requirements for activities associated with the transport of information system media in accordance with the organizational assessment of risk to include the flexibility to define different record-keeping methods for different types of media transport as part of an overall system of transport-related records.	
(3)	The organization employs an identified custodian throughout the transport of information system media.	
	Enhancement Supplemental Guidance: Custodial responsibilities can be transferred from one individual to another as long as an unambiguous custodian is identified at all times.	
(4)	The organization employs cryptographic mechanisms to protect the confidentiality and integrity of information stored on digital media during transport outside of controlled areas.	
	Enhancement Supplemental Guidance: This control enhancement also applies to mobile devices. Mobile devices include portable storage media (e.g., USB memory sticks, external hard disk drives) and portable computing and communications devices with storage capability (e.g., notebook/laptop computers, personal digital assistants, cellular telephones). Related control: MP-4. Related controls: MP-2; SC-13.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.7 Maintain strict control over the internal or external distribution of any kind of media. 9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked.	
MP-6	**MEDIA SANITIZATION**	Previous SEC 501-06 Control References: 4.6.2.16
	Control: The organization sanitizes information system media, both digital and non-digital, prior to disposal, release out of organizational control, or release for reuse.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	
(1)	The organization tracks, documents, and verifies media sanitization and disposal actions.	
(2)	The organization tests sanitization equipment and procedures to verify correct performance 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).	
(3)	The organization sanitizes portable, removable storage devices prior to connecting such devices to the information system.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: Portable, removable storage devices (e.g., thumb drives, flash drives, external storage devices) can be the source of malicious code insertions into organizational information systems. Many of these devices are obtained from unknown sources and may contain various types of malicious code that can be readily transferred to the information system through USB ports or other entry portals. While scanning such devices is always recommended, sanitization provides additional assurance that the device is free of all malicious code to include code capable of initiating zero-day attacks. Organizations consider sanitization of portable, removable storage devices, for example, when such devices are first purchased from the manufacturer or vendor prior to initial use or when the organization loses a positive chain of custody for the device. An organizational assessment of risk guides the specific circumstances for employing the sanitization process. Related control: SI-3.	
(6)	The organization destroys information system media that cannot be sanitized.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.10 Destroy media when it is no longer needed for business or legal reasons as follows: 9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. 9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	
MP-6-COV	**MEDIA SANITIZATION (COV)**	Previous SEC 501-06 Control References: 10.2.2.3
	Control: 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).	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.10 Destroy media when it is no longer needed for business or legal reasons as follows: 9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed. 9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	
2.11	***FAMILY** : PHYSICAL AND ENVIRONMENTAL PROTECTION*	***CLASS:** OPERATIONAL*
PE-1-COV	**PHYSICAL AND ENVIRONMENTAL PROTECTION (COV)**	Previous SEC 501-06 Control References: 7.2.2/10.2.2.1
1	**Control: Identify whether IT assets may be removed from premises that house IT systems and data, and if so, identify the controls over such removal.**	
2	Design safeguards, commensurate with risk, to protect against human, natural, and environmental threats.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-2	**PHYSICAL ACCESS AUTHORIZATIONS**	Previous SEC 501-06 Control References: 7.2
	Control: The organization:	
a.	Develops and keeps current a list of personnel with authorized access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible);	
b.	Issues authorization credentials;	
c.	Reviews and approves the access list and authorization credentials periodically, removing from the access list personnel no longer requiring access.	
	Supplemental Guidance: Authorization credentials include, for example, badges, identification cards, and smart cards. This control includes the Department of General Services issuance of credentials. Related control: PE-3, PE-4.	
	DMV-Specific Requirements: The following restrictions apply to IT facilities/areas at DMV: 1. The IT Security Director shall perform annual reviews to ensured IT restricted space complies with the requirements in this control. 2. The IT Security Director shall periodically review the list of persons with authorized access. 3. Only individuals with a business need will have authorized access to IT restricted space. 4. Any employee or contractor that no longer has a business need to enter IT restricted space will have their access immediately removed. 5. Approved identification cards with photo are required for all employees and contractors with an ongoing, recurring business need to enter the IT restricted area and this ID shall be displayed at all times while in the building. 6. All personnel are subject to screening by law enforcement and/or security personnel to include the examination of photo identification and the physical examination of all personal items to include, but not limited to, coats, jackets, handbags, personal organizers, briefcases, computer laptops and other personal electronic devices. PCI 9.1 VITA PE-2	
	Control Enhancements for Sensitive Systems:	
(1)	The organization authorizes physical access to the facility where the information system resides based on position or role.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
PE-3	**PHYSICAL ACCESS CONTROL**	Previous SEC 501-06 Control References: 7.2.5
	Control: The organization:	
a.	Enforces physical access authorizations for all physical access points (including designated entry/exit points) to the facility where the information system resides (excluding those areas within the facility officially designated as publicly accessible);	
b.	Verifies individual access authorizations before granting access to the facility;	
c.	Controls entry to the facility containing the information system using physical access devices and/or guards;	
d.	Controls access to areas officially designated as publicly accessible in accordance with the organization's assessment of risk;	
e.	Secures keys, combinations, and other physical access devices;	
f.	Inventories physical access devices once a year at a minimum; and	
g.	Changes combinations and keys once every two-years at a minimum and when keys are lost, combinations are compromised, or individuals are transferred or terminated.	
	Supplemental Guidance: The organization determines the types of guards needed, for example, professional physical security staff or other personnel such as administrative staff or information system users, as deemed appropriate. Physical access devices include, for example, keys, locks, combinations, and card readers. Workstations and associated peripherals connected to (and part of) an organizational information system may be located in areas designated as publicly accessible with access to such devices being safeguarded. Related controls: MP-2, MP-4, PE-2.	
	DMV-Specific Requirements: The following restrictions apply to IT facilities/areas at DMV: 1. When possible, entrances to IT restricted space are electronically controlled with the capability of providing an audit trail. PCI 9.1, 9.1.3 VITA PE-3	
	Control Enhancements for Sensitive Systems:	
(1)	The organization enforces physical access authorizations to the information system independent of the physical access controls for the facility.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: This control enhancement applies to server rooms, media storage areas, communications centers, or any other areas within an organizational facility containing large concentrations of information system components. The intent is to provide additional physical security for those areas where the organization may be more vulnerable due to the concentration of information system components. Security requirements for facilities containing organizational information systems that process, store, or transmit Sensitive Compartmented Information (SCI) are consistent with applicable laws, directives, policies, regulations, standards, and guidance. See also PS-3, security requirements for personnel access to SCI.	
(3)	The organization guards, alarms, and monitors every physical access point to the facility where the information system resides 24 hours per day, 7 days per week.	
(6)	The organization employs a penetration testing process that includes annual, unannounced attempts to bypass or circumvent security controls associated with physical access points to the facility.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. 9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines.	
PE-4	**ACCESS CONTROL FOR TRANSMISSION MEDIUM**	Previous SEC 501-06 Control References: 7.2.5 Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization controls physical access to information system distribution and transmission lines within organizational facilities.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines. 12.3.6 Acceptable network locations for the technologies.	
PE-5	**ACCESS CONTROL FOR OUTPUT DEVICES**	Previous SEC 501-06 Control References: 7.2.5
	Control: The organization controls physical access to information system output devices to prevent unauthorized individuals from obtaining the output.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Monitors, printers, and audio devices are examples of information system output devices.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	
PE-6	**MONITORING PHYSICAL ACCESS**	Previous SEC 501-06 Control References: 7.2.6
	Control: The organization:	
a.	Monitors physical access to the information system to detect and respond to physical security incidents;	
b.	Reviews physical access logs once every 60-days at a minimum; and	
c.	Coordinates results of reviews and investigations with the organization's incident response capability.	
	Supplemental Guidance: Investigation of and response to detected physical security incidents, including apparent security violations or suspicious physical access activities, are part of the organization's incident response capability and must be reported to Commonwealth Security.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization monitors real-time physical intrusion alarms and surveillance equipment.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment. 9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	
PE-7	**VISITOR CONTROL**	Previous SEC 501-06 Control References: 8.2.2.2
	Control: The organization controls physical access to the information system by authenticating visitors before authorizing access to the facility where the information system resides other than areas designated as publicly accessible.	
	Supplemental Guidance: Individuals (to include organizational employees, contract personnel, and others) with permanent authorization credentials for the facility are not considered visitors.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization escorts visitors and monitors visitor activity, when required.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. 9.3 Make sure all visitors are handled as follows: 9.3.1 Authorized before entering areas where cardholder data is processed or maintained. 9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel. 9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration. 9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	
PE-8	**ACCESS RECORDS (VISITOR)**	Previous SEC 501-06 Control References: 7.2.6/7.2.7
	Control: The organization:	
a.	Maintains visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible); and	
b.	Reviews visitor access records once every 90-days at a minimum.	
	Supplemental Guidance: Visitor access records include, for example, name/organization of the person visiting, signature of the visitor, form(s) of identification, date of access, time of entry and departure, purpose of visit, and name/organization of person visited.	
	Control Enhancements for Sensitive Systems:	
(2)	The organization maintains a record of all physical access, both visitor and authorized individuals.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible. 9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	
PE-9	**POWER EQUIPMENT AND POWER CABLING**	Previous SEC 501-06 Control References: 7.2
	Control: The organization protects power equipment and power cabling for the information system from damage and destruction.	
	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-10	**EMERGENCY SHUTOFF**	Previous SEC 501-06 Control References: 7.2
	Control: The organization:	
a.	Provides the capability of shutting off power to the information system or individual system components in emergency situations;	
b.	Places emergency shutoff switches or devices in organization-defined location by information system or system component to facilitate safe and easy access for personnel; and	
c.	Protects emergency power shutoff capability from unauthorized activation.	
	Supplemental Guidance: This control applies to facilities containing concentrations of information system resources, for example, data centers, server rooms, and mainframe computer rooms.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-11	**EMERGENCY POWER**	Previous SEC 501-06 Control References: 7.2
	Control: The organization provides a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss.	
	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-13	**FIRE PROTECTION**	Previous SEC 501-06 Control References: 7.2
	Control: The organization employs and maintains fire suppression and detection devices/systems for the information system that are supported by an independent energy source.	
	Supplemental Guidance: Fire suppression and detection devices/systems include, for example, sprinkler systems, handheld fire extinguishers, fixed fire hoses, and smoke detectors. This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-14	**TEMPERATURE AND HUMIDITY CONTROLS**	Previous SEC 501-06 Control References: 7.2
	Control: The organization:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
a.	Maintains temperature and humidity levels within the facility where the information system resides at a temperature of 72 degrees F (+/- 2 F) and a relative humidity of 45% (+/- 5%); and	
b.	Monitors temperature and humidity levels on a daily basis.	
	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-15	**WATER DAMAGE PROTECTION**	Previous SEC 501-06 Control References: 7.2 Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization protects the information system from damage resulting from water leakage by providing master shutoff valves that are accessible, working properly, and known to key personnel.	
	Supplemental Guidance: This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PE-18	**LOCATION OF INFORMATION SYSTEM COMPONENTS**	Previous SEC 501-06 Control References: 3.4.2
	Control: The organization positions information system components within the facility to minimize potential damage from physical and environmental hazards and to minimize the opportunity for unauthorized access.	
	Supplemental Guidance: Physical and environmental hazards include, for example, flooding, fire, tornados, earthquakes, hurricanes, acts of terrorism, vandalism, electromagnetic pulse, electrical interference, and electromagnetic radiation. Whenever possible, the organization also considers the location or site of the facility with regard to physical and environmental hazards. In addition, the organization considers the location of physical entry points where unauthorized individuals, while not being granted access, might nonetheless be in close proximity to the information system and therefore, increase the potential for unauthorized access to organizational communications (e.g., through the use of wireless sniffers or microphones). This control, to include any enhancements specified, may be satisfied by similar requirements fulfilled by another organizational entity other than the information security program. Organizations avoid duplicating actions already covered.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: The following restrictions apply to IT facilities/areas at DMV: 1. The IT Security Director manages security of IT restricted space 2. Planned changes for IT restricted spaces require that physical security is with the IT Security Director during the design phase. PCI 12.3.6 VITA PE-18	
	Control Enhancements for Sensitive Systems:	
(1)	The organization plans the location or site of the facility where the information system resides with regard to physical and environmental hazards and for existing facilities, considers the physical and environmental hazards in its risk mitigation strategy.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.3.6 Acceptable network locations for the technologies.	
2.12	***FAMILY:*** *PLANNING*	***CLASS:*** *MANAGEMENT*
PL-2	**SYSTEM SECURITY PLAN**	Previous SEC 501-06 Control References: 4.2/ 4.2.2.4
	Control: The organization:	
a.	Develops a security plan for the information system that:	
	- Is consistent with the organization's enterprise architecture;	
	- Explicitly defines the authorization boundary for the system;	
	- Describes the operational context of the information system in terms of missions and business processes;	
	- Provides the security categorization of the information system including supporting rationale;	
	- Describes the operational environment for the information system;	
	- Describes relationships with or connections to other information systems;	
	- Provides an overview of the security requirements for the system;	
	- Describes the security controls in place or planned for meeting those requirements including a rationale for the tailoring and supplementation decisions; and	
	- Is reviewed and approved by the authorizing official or designated representative prior to plan implementation;	
b.	Reviews the security plan for the information system every three years, or more often if necessary (i.e. due to material change), and resubmit the IT System Security Plan to the Agency Head or designated ISO for approval.; and	
c.	Updates the plan to address changes to the information system/environment of operation or problems identified during plan implementation or security control assessments.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The security plan contains sufficient information (including specification of parameters for assignment and selection statements in security controls either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a subsequent determination of risk to organizational operations and assets, individuals, other organizations, and the Commonwealth if the plan is implemented as intended. Related controls: None	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PL-2-COV	**SYSTEM SECURITY PLAN (COV)**	Previous SEC 501-06 Control References: 4.2.2
	Control: The organization:	
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.	
2	Submit the IT System Security Plan to the Agency Head or designated ISO for approval.	
3	Plan, document, and implement additional 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.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	
	PCI compliance: PCI-DSS has no requirement for this control.	
PL-4	**RULES OF BEHAVIOR**	Previous SEC 501-06 Control References: 8.3.2.7.g
	Control: The organization:	
a.	Establishes and makes readily available to all information system users, the rules that describe their responsibilities and expected behavior with regard to information and information system usage; and	
b.	Receives signed acknowledgment from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to information and the information system.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	
(1)	The organization includes in the rules of behavior, explicit restrictions on the use of social networking sites, posting information on commercial websites, and sharing information system account information.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data. 12.3.5 Acceptable uses of the technology. 12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	
PL-4-COV	**RULES OF BEHAVIOR (COV)**	Previous SEC 501-06 Control References: 8.5.2
1	**Control: 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.**	
2	Prohibit users from:	
a.	Installing or using proprietary encryption hardware/software on Commonwealth systems;	
b.	Tampering with security controls configured on COV workstations;	
c.	Installing personal software on a Commonwealth 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).	
3	Prohibit the storage, use or transmission of copyrighted and licensed materials on COV systems unless the COV owns the materials or COV has otherwise complied with licensing and copyright laws governing the materials.	
4	The organization should consult with legal counsel when considering adopting an email disclaimer. Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
5	The following is the approved e-signature and email disclaimer for DMV: To maintain a uniform signature, employee email signatures should use Arial 10 point font and include the following information: Your Name Title Virginia Department of Motor Vehicles CSC/MCSC/DMV Direct/Work Center Name Address City, State Zip Office: (XXX) XXX-XXXX Fax: (XXX) XXX-XXXX Cell: (XXX) XXX-XXXX (if applicable) Email address Visit us at www.dmvNOW.com DMV is going green. Please consider the environment before printing this email. Confidentiality Statement: The information contained in this message and any attachments may be privileged and/or confidential and it is intended only for the use of the individual or entity named above. If you are not the intended recipient, you are hereby notified that you are prohibited from disseminating, distributing, or copying the information contained in this message or any attachments. If you have received this message in error, please notify the sender immediately and destroy all copies of the original message and any attachments.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: For all personnel with access to Agency information or systems: 1. All personnel who handle sensitive information shall take appropriate steps to conceal it from non-authorized parties. 2. Any sensitive or confidential Agency information shall not be discussed in public places or non-secure DMV office space (e.g., restrooms, cafeteria, and hallways) where the possibility of unauthorized personnel overhearing the conversation exists. 3. If sensitive data is discussed in a meeting, seminar, lecture, or related presentation, the speaker shall clearly emphasize its sensitivity and request information only be shared with those specifically authorized. 4. Sensitive information recorded on erasable surfaces including, but not limited to, black boards and white boards, shall be definitively erased before the authorized recipients of this information leave the area. 5. All users shall not leave their individual computer, workstation, or terminal unattended without logging out, locking their computer or invoking a password-protected screen saver. 6. All users shall log off their computers when left unattended for an extended period; overnight, weekends or leave. The IT Security Director shall or shall require its service provider (VITA) ensure that the following requirements are met for protecting COV data when using telephones: 1. Employees must never discuss sensitive information on unencrypted cordless or cellular telephones. 2. Employees must not record messages containing sensitive information on answering machines or voice mail systems. 3. Employees must, unless they are on vacation or sick leave, check their voice mail at least once every business day. VITA PL-4-COV	
	Security Tools and Components: For all personnel with access to Agency systems: 1. All DMV users, including employees, contractors, consultants, vendors and all other personnel with access to DMV information systems and networks, shall not acquire, possess, trade, or use hardware or software tools that could be employed to evaluate or compromise information systems security unless specifically authorized by the IT Security Director. Examples of such tools include, but are not limited to, those which defeat software copy protection, discover secret passwords, identify security vulnerabilities, or decrypt encrypted files. 2. No user shall disable, bypass, turn off, or disconnect any critical components of DMV information security infrastructure without prior approval from the IT Security Director. This applies to all IT hardware and software, either operating on the COV/DMV network or standalone. It includes but is not limited to workstations, servers, peripheral devices, routers, switches, firewalls, hubs and storage, as well as all software used to operate, manage, protect or monitor the equipment. VITA PL-4-COV	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.3.5 Acceptable uses of the technology.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
PL-6	**SECURITY-RELATED ACTIVITY PLANNING**	Previous SEC 501-06 Control References: None
	Control: The organization plans and coordinates security-related activities affecting the information system before conducting such activities in order to reduce the impact on organizational operations (i.e., mission, functions, image, and reputation), organizational assets, and individuals.	
	Supplemental Guidance: Security-related activities include, for example, security assessments, audits, system hardware and software maintenance, and contingency plan testing/exercises. Organizational advance planning and coordination includes both emergency and nonemergency (i.e., planned or non-urgent unplanned) situations.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
2.13	***FAMILY:*** *PERSONNEL SECURITY*	***CLASS:*** *OPERATIONAL*
PS-2	**POSITION CATEGORIZATION**	Previous SEC 501-06 Control References: 2.2 Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization:	
a.	Assignment of privileges/access to individuals shall be based on job classification and function (role based). Individual unique identity shall map to one or more identified roles.	
b.	Access to objects by default shall be restricted via an access control mechanism. Access shall be specifically granted to provide explicit access to objects within any information system.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 7.1.2 Assignment of privileges is based on individual personnel's job classification and function	
PS-3	**PERSONNEL SCREENING**	Previous SEC 501-06 Control References: 8.2.2.1
	Control: The organization:	
a.	Screens individuals prior to authorizing access to the information system.	
	Supplemental Guidance: Refer to Department of Human Resource Management (DHRM) policy.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. Examples of background checks include previous employment history, criminal record, credit history and reference checks.	
PS-4	**PERSONNEL TERMINATION**	Previous SEC 501-06 Control References: 8.2.2
	Control: The organization, upon termination of individual employment:	
a.	Terminates information system access;	
b.	Conducts exit interviews;	
c.	Retrieves all security-related organizational information system-related property; and	
d.	Retains access to organizational information and information systems formerly controlled by terminated individual.	
	Supplemental Guidance: Refer to Department of Human Resource Management (DHRM) policy and Library of Virginia (LVA) requirements.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.4 Immediately revoke access for any terminated users.	
PS-5	**PERSONNEL TRANSFER**	Previous SEC 501-06 Control References: 8.2.2.4
	Control: The organization reviews logical and physical access authorizations to information systems/facilities when personnel are reassigned or transferred to other positions within the organization and initiates the System Access Request Form (SAR13) process for logical access in a timely manner. In addition, the HRO 14 Employment Termination Checklist is used for terminations. The appropriate level of physical access, new/modified/removed, will be requested from the assigned person in the facility.	
	Supplemental Guidance: This control applies when the reassignment or transfer of an employee is permanent or of such an extended duration as to make the actions warranted. In addition, the organization defines the actions appropriate for the type of reassignment or transfer; whether permanent or temporary. Actions that may be required when personnel are transferred or reassigned to other positions within the organization include, for example: (i) returning old and issuing new keys, identification cards, and building passes; (ii) closing previous information system accounts and establishing new accounts; (iii) changing information system access authorizations; and (iv) providing for access to official records to which the employee had access at the previous work location and in the previous information system accounts.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: PCI-DSS has no requirement for this control.	
PS-6	**ACCESS AGREEMENTS**	Previous SEC 501-06 Control References: 5.2.2/8.4.2.8
	Control: The organization:	
a.	Ensures that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access; and	
b.	Reviews/updates the access agreements once a year at a minimum or whenever the employment status of an individual changes.	
	Supplemental Guidance: Access agreements include, for example, nondisclosure agreements, acceptable use agreements, rules of behavior, and conflict-of-interest agreements. Signed access agreements include an acknowledgement that individuals have read, understand, and agree to abide by the constraints associated with the information system to which access is authorized. Electronic signatures are acceptable for use in acknowledging access agreements unless specifically prohibited by organizational policy. Related control: PL-4.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data. 12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	
PS-7	**THIRD-PARTY PERSONNEL SECURITY**	Previous SEC 501-06 Control References: 8.2.2
	Control: The organization:	
a.	Establishes personnel security requirements including security roles and responsibilities for third-party providers;	
b.	Documents personnel security requirements; and	
c.	Monitors provider compliance.	
	Supplemental Guidance: Third-party providers include, for example, service bureaus, contractors, and other organizations providing information system development, information technology services, outsourced applications, and network and security management. The organization explicitly includes personnel security requirements in acquisition-related documents.	
	Control: The organization employs a formal sanctions process for personnel failing to comply with established information security policies and procedures.	
	Supplemental Guidance: Refer to Department of Human Resource Management (DHRM) policy.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
2.14	***FAMILY:*** *RISK ASSESSMENT*	***CLASS:*** *MANAGEMENT*
RA-2	**SECURITY CATEGORIZATION**	Previous SEC 501-06 Control References: 2.5
	Control: The organization:	
a.	Categorizes information and the information system in accordance Commonwealth policies and procedures	
b.	Documents the security categorization results (including supporting rationale) in the security plan for the information system; and	
c.	Ensures the security categorization decision is reviewed and approved by the authorizing official or authorizing official designated representative.	
	Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective security categorization. Security categorization describes the potential adverse impacts to organizational operations, organizational assets, and individuals should the information and information system be compromised through a loss of confidentiality, integrity, or availability.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Guidance: IT System and Data Sensitivity Classification requirements identify the steps necessary to classify IT systems and data according to their sensitivity with respect to the following three criteria: • Confidentiality, which addresses sensitivity to unauthorized disclosure; • Integrity, which addresses sensitivity to unauthorized modification; and • Availability, which addresses sensitivity to outages. Sensitive Data is any data that, if compromised with respect to confidentiality, integrity, and/or availability, could have a material adverse effect on COV interests, the conduct of DMV programs, or the privacy to which individuals are entitled. Data sensitivity is directly proportional to the materiality of a compromise of the data with respect to these criteria. DMV must classify each IT system by sensitivity according to the most sensitive data that the IT system stores, processes, or transmits. Sensitive Data as Defined by DMV Examples of sensitive data include: 1. Any personal data which may subject an employee or customer of DMV to the threat of identity theft and personal liability, financial or otherwise. This includes, but is not limited to, all personally identifiable information maintained by DMV about an individual, including, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother's maiden name, photograph, biometric records, ancestry, religion, political ideology, etc., including any other personal information which is linked or linkable to an individual. 2. Proprietary research data. 3. Certain confidential proprietary data. 4. Network diagrams and IP addresses.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Requirements The IT Security Director shall: 1. Identify or require that the Data Owner identify the type(s) of data handled by each DMV IT system. 2. Determine or require that the Data Owner determine whether each type of data is also subject to other regulatory requirements. Example: Some COV IT systems may handle data subject to legal or business requirements such as the Health Insurance Portability and Accountability Act of 1996 (HIPAA); IRS 1075; the Privacy Act of 1974; Payment Card Industry (PCI); the Rehabilitation Act of 1973, § 508, Federal National Security Standards, etc. 3. Determine or require that the Data Owner determine the potential damages to DMV 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. **Example:** Data Owners should construct a table using *IT System and Data Sensitivity Classification Template* shown in the ***Forms*** section of this document. Data Owners must classify sensitivity requirements of all types of data. 4. Any data type with one or more HIGH sensitivity rating in any of the three classifications shall be classified "sensitive" for the purposes of this standard. **Note:** The IT Security Director shall classify IT systems as sensitive even if a type of data handled by the IT system has a sensitivity of moderate on the criteria of confidentiality, integrity, and availability.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	5. Review IT system and data classifications with the Commissioner or Assistant Commissioner/CIO and obtain Commissioner's or Assistant Commissioner/CIO's approval of these classifications. 6. Verify and validate that all DMV IT systems and data have been classified for sensitivity. 7. Communicate approved IT system and data classifications to System Owners, Data Owners, and end-users. 8. Require that DMV 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 Commissioner identifying the business case, risks, mitigating logical and physical controls, and any residual risk. 9. Use the information documented in the sensitivity classification as a primary input to the Risk Assessment process.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components. 9.7.1 Classify media so the sensitivity of the data can be determined.	
RA-3	**RISK ASSESSMENT**	Previous SEC 501-06 Control References: 2.7/2.7.2/4.2.3.7
	Control: The organization:	
a.	Conducts an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits;	
b.	Documents risk assessment results in a Risk Assessment Report;	
c.	Reviews risk assessment results once a year at a minimum; and	
d.	Updates the risk assessment once a year at a minimum or whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities), or other conditions that may impact the security state of the system.	
	Supplemental Guidance: A clearly defined authorization boundary is a prerequisite for an effective risk assessment. Risk assessments take into account vulnerabilities, threat sources, and security controls planned or in place to determine the level of residual risk posed to organizational operations and assets, individuals, other organizations, and the Commonwealth based on the operation of the information system. Risk assessments also take into account risk posed to organizational operations, organizational assets, or individuals from external parties (e.g., service providers, contractors operating information systems on behalf of the organization, individuals accessing organizational information systems, outsourcing entities).	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: Purpose Risk Assessment requirements delineate the steps agencies must take for each IT system classified as sensitive to: - Identify potential threats to an IT system and the environment in which it operates; - Determine the likelihood that threats will materialize; - Identify and evaluate vulnerabilities; and - Determine the loss impact if one or more vulnerabilities are exploited by a potential threat. Requirements For each IT system classified as sensitive, the data-owning agency shall: 1. Conduct and document a RA of the IT system as needed, but not less than once every three years. 2. Conduct and document an annual self-assessment to determine the continued validity of the RA. **Note:** In addition, in agencies that own both sensitive IT systems and IT systems that are exempt from the requirements of this Standard, the agency's RAs must include consideration of the added risk to sensitive IT systems from the exempt 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. PCI 12.1.2 VITA RA-3	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment. 12.1.3 Includes a review at least annually and updates when the environment changes.	
RA-5	**VULNERABILITY SCANNING**	Previous SEC 501-06 Control References: 4.7.2.11
	Control: The organization:	
a.	Scans for vulnerabilities in the information system and hosted applications once every 90-days at a minimum and when new vulnerabilities potentially affecting the system/applications are identified and reported;	
b.	Employs vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:	
	Enumerating platforms, software flaws, and improper configurations;	
	Formatting and making transparent, checklists and test procedures; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Measuring vulnerability impact.	
c.	Analyzes vulnerability scan reports and results from security control assessments;	
d.	Remediates legitimate vulnerabilities within 14 days in accordance with an organizational assessment of risk; and	
e.	Shares information obtained from the vulnerability scanning process and security control assessments with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies).	
	Supplemental Guidance: The security categorization of the information system guides the frequency and comprehensiveness of the vulnerability scans. Vulnerability analysis for custom software and applications may require additional, more specialized techniques and approaches (e.g., web-based application scanners, source code reviews, source code analyzers). Vulnerability scanning includes scanning for specific functions, ports, protocols, and services that should not be accessible to users or devices and for improperly configured or incorrectly operating information flow mechanisms. The organization considers using tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and that use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities. Related controls: CA-2, CM-6, RA-3, SI-2.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs vulnerability scanning tools that include the capability to readily update the list of information system vulnerabilities scanned.	
(2)	The organization updates the list of information system vulnerabilities scanned once every 180-days at a minimum or when new vulnerabilities are identified and reported.	
(3)	The organization employs vulnerability scanning procedures that can demonstrate the breadth and depth of coverage (i.e., information system components scanned and vulnerabilities checked).	
(4)	The organization attempts to discern what information about the information system is discoverable by adversaries.	
(5)	The organization includes privileged access authorization to the organization-identified information system components for selected vulnerability scanning activities to facilitate more thorough scanning.	
(9)	The organization employs an independent penetration agent or penetration team to: (a) Conduct a vulnerability analysis on the information system; and (b) Perform penetration testing on the information system based on the vulnerability analysis to determine the exploitability of identified vulnerabilities.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: A standard method for penetration testing includes: (i) pre-test analysis based on full knowledge of the target information system; (ii) pre-test identification of potential vulnerabilities based on pre-test analysis; and (iii) testing designed to determine exploitability of identified vulnerabilities. Detailed rules of engagement are agreed upon by all parties before the commencement of any penetration testing scenarios. Related control: SA-12.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. 6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 11.2.1 Perform quarterly internal vulnerability scans. 11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). 11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following: 11.3.1 Network-layer penetration tests. 11.3.2 Application-layer penetration tests. NOTE: The requirement for ASV-performed vulnerability scans (PCI 11.2.2) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control RA-5's requirements apply to all other DMV systems.	
RA-5-COV	**VULNERABILITY SCANNING (COV)**	Previous SEC 501-06 Control References: 4.7.2.11
	Control: The organization:	
	Scans for vulnerabilities in the sensitive information systems and hosted applications at least once every 90-days and when new vulnerabilities potentially affecting the system/applications are identified and reported;	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications 11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the network (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades). 11.2.1 Perform quarterly internal vulnerability scans. 11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC). NOTE: The requirement for ASV-performed vulnerability scans (PCI 11.2.2) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control RA-5-COV's requirements apply to all other DMV systems.	
2.15	***FAMILY:*** *SYSTEM AND SERVICES ACQUISITION*	***CLASS:*** *MANAGEMENT*
SA-2	**ALLOCATION OF RESOURCES**	Previous SEC 501-06 Control References: None
	Control: The organization:	
a.	Includes a determination of information security requirements for the information system in mission/business process planning;	
b.	Determines, documents, and allocates the resources required to protect the information system as part of its capital planning and investment control process; and	
c.	Establishes a discrete line item for information security in organizational programming and budgeting documentation.	
	Supplemental Guidance: Related controls: PM-3, PM-11.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-3	**LIFE CYCLE SUPPORT**	Previous SEC 501-06 Control References: 4.6
	Control: The organization:	
a.	Manages the information system using a system development life cycle methodology that includes information security considerations;	
b.	Defines and documents information system security roles and responsibilities throughout the system development life cycle; and	
c.	Identifies individuals having information system security roles and responsibilities.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Related control: PM-7.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.4.2 Separation of duties between development/test and production environments. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes; as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	
SA-3-COV-1	**LIFE CYCLE SUPPORT (COV-1)**	Previous SEC 501-06 Control References: 4.6
	Control: Each Agency shall:	
1	Project Initiation	
a.	Perform an initial risk analysis based on the known requirements and the business objectives to provide high-level security guidelines for the system developers.	
b.	Classify the types of data (see IT System and Data Sensitivity Classification) that the IT system will process and the sensitivity of the proposed IT system.	
c.	Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.	
d.	Develop an initial IT System Security Plan (see IT System Security Plans) that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.	
e.	Project Definition	
f.	Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.	
g.	Incorporate IT security requirements in IT system design specifications.	
h.	Verify that the IT system development process designs, develops, and implements IT security controls that meet information security requirements in the design specifications.	
i.	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.	
j.	Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.	
2	Implementation	
a.	Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.	
b.	Conduct a Risk Assessment (see Risk Assessment) to assess the risk level of the IT application system.	
c.	Require that the system comply with all relevant Risk Management requirements in this Standard.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
d.	Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against information security risks, and comply with the other requirements (see IT Systems Security Plans) of this document.	
3	Disposition	
a.	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.	
b.	Require that electronic media is sanitized prior to disposal, as documented (see Data Storage Media Protection), so that all data is removed from the IT system.	
c.	Verify the disposal of hardware and software 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).	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 3.1.1 Implement a data retention and disposal policy that includes: § Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. § Processes for secure deletion of data when no longer needed. § Specific retention requirements for cardholder data. § A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements. 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes; as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	
SA-3-COV-2	**LIFE CYCLE SUPPORT (COV-2)**	Previous SEC 501-06 Control References: 4.7
	Control: Each agency ISO is accountable for ensuring the following steps are documented and followed:	
1	Application Planning	
a.	Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.	
b.	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.	
c.	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.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
d.	Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication, access control, and logging requirements. When planning to use, process or store sensitive information in an application, agencies must address the following design criteria:	
i.	Encrypted communication channels shall be established for the transmission of sensitive information;	
ii.	Sensitive information shall not be visibly transmitted between the client and the application; and	
iii.	Sensitive information shall not be stored in hidden fields that are part of the application interface.	
2	Application Development	
a.	The following requirements represent a minimal set of coding practices, which shall be applied to all applications under development.	
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.	
c.	Session Management - Any user sessions created by an application shall support an automatic inactivity timeout function.	
d.	Data storage shall be separated either logically or physically, from the application interface (i.e., design two or three tier architectures where possible).	
e.	Agencies shall not use or store sensitive data in non-production environments (i.e., a development or test environment that does not have security controls equivalent to the production environment).	
f.	Input Validation – All application input shall be validated irrespective of source. Input validation should always consider both expected and unexpected input, and not block input based on arbitrary criteria.	
g.	Default Deny – Application access control shall implement a default deny policy, with access explicitly granted	
h.	Principle of Least Privilege – All processing shall be performed with the least set of privileges required.	
i.	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.	
j.	Configure applications to clear the cached data and temporary files upon exit of the application or logoff of the system.	
3	Production and Maintenance	
a.	Production applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
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.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. 6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following: 6.4.1 Separate development/test and production environments. 6.4.3 Production data (live PANs) are not used for testing or development. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes; as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. 6.5.4 Insecure communications. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. 7.2.3 Default "deny-all" setting. For sensitive, internet-facing applications only: 11.2.3 Perform internal and external scans after any significant change	
SA-4	**ACQUISITIONS**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The organization includes the following requirements and/or specifications, explicitly or by reference, in information system acquisition contracts based on an assessment of risk and in accordance with applicable laws, directives, policies, regulations, and standards:	
a.	Security functional requirements/specifications;	
b.	Security-related documentation requirements; and	
c.	Developmental and evaluation-related assurance requirements.	
	Supplemental Guidance: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control Enhancements for Sensitive Systems:	
(1)	The organization requires in acquisition documents that vendors/contractors provide information describing the functional properties of the security controls to be employed within the information system, information system components, or information system services in sufficient detail to permit analysis and testing of the controls.	
(2)	The organization requires in acquisition documents that vendors/contractors provide information describing the design and implementation details of the security controls to be employed within the information system, information system components, or information system services (including functional interfaces among control components) in sufficient detail to permit analysis and testing of the controls.	
(5)	The organization requires in acquisition documents, that information system components are delivered in a secure, documented configuration, and that the secure configuration is the default configuration for any software reinstalls or upgrades.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	
SA-5	**INFORMATION SYSTEM DOCUMENTATION**	Previous SEC 501-06 Control References: 4.3.2/2.4.2
	Control: The organization:	
a.	Obtains, protects as required, and makes available to authorized personnel, administrator documentation for the information system that describes:	
	- Secure configuration, installation, and operation of the information system;	
	- Effective use and maintenance of security features/functions; and	
	- Known vulnerabilities regarding configuration and use of administrative (i.e., privileged) functions; and	
b.	Obtains, protects as required, and makes available to authorized personnel, user documentation for the information system that describes:	
	- User-accessible security features/functions and how to effectively use those security features/functions;	
	- Methods for user interaction with the information system, which enables individuals to use the system in a more secure manner; and	
	- User responsibilities in maintaining the security of the information and information system; and	
c.	Documents attempts to obtain information system documentation when such documentation is either unavailable or nonexistent.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The inability of the organization to obtain necessary information system documentation may occur, for example, due to the age of the system and/or lack of support from the vendor/contractor. In those situations, organizations may need to recreate selected information system documentation if such documentation is essential to the effective implementation and/or operation of security controls. Service providers provide assurance that this control is met where applicable.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the functional properties of the security controls employed within the information system with sufficient detail to permit analysis and testing.	
(2)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the security-relevant external interfaces to the information system with sufficient detail to permit analysis and testing.	
(3)	The organization obtains, protects as required, and makes available to authorized personnel, vendor/manufacturer documentation that describes the high-level design of the information system in terms of subsystems and implementation details of the security controls employed within the system with sufficient detail to permit analysis and testing.	
	Enhancement Supplemental Guidance: An information system can be partitioned into multiple subsystems.	
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-6	**SOFTWARE USAGE RESTRICTIONS**	Previous SEC 501-06 Control References: 8.4.2.5
	Control: The organization:	
a.	Uses software and associated documentation in accordance with contract agreements and copyright laws;	
b.	Employs tracking systems for software and associated documentation protected by quantity licenses to control copying and distribution; and	
c.	Controls and documents the use of peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorized distribution, display, performance, or reproduction of copyrighted work.	
	Supplemental Guidance: Tracking systems can include, for example, simple spreadsheets or fully automated, specialized applications depending on the needs of the organization.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-6-COV	**SOFTWARE USAGE RESTRICTIONS (COV)**	Previous SEC 501-06 Control References: 10.3.2
	Control: 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 only agency approved software and service provider approved systems management software on IT systems.	
2	Assess periodically whether all software is used in accordance with license agreements.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-7	**USER-INSTALLED SOFTWARE**	Previous SEC 501-06 Control References: 8.4.2.5
	Control: The organization enforces explicit rules governing the installation of software by users.	
	Supplemental Guidance: If provided the necessary privileges, users have the ability to install software. The organization identifies what types of software installations are permitted (e.g., updates and security patches to existing software) and what types of installations are prohibited (e.g., software whose pedigree with regard to being potentially malicious is unknown or suspect). Related control: CM-2.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-8	**SECURITY ENGINEERING PRINCIPLES**	Previous SEC 501-06 Control References: 4.7.2
	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.	
	Supplemental Guidance: The application of security engineering principles is primarily targeted at new development information systems or systems undergoing major upgrades and is integrated into the system development life cycle. For legacy information systems, the organization applies security engineering principles to system upgrades and modifications to the extent feasible, given the current state of the hardware, software, and firmware within the system. Examples of security engineering principles include, for example: (i) developing layered protections; (ii) establishing sound security policy, architecture, and controls as the foundation for design; (iii) incorporating security into the system development life cycle; (iv) delineating physical and logical security boundaries; (v) ensuring system developers and integrators are trained on how to develop secure software; (vi) tailoring security controls to meet organizational and operational needs; and (vii) reducing risk to acceptable levels, thus enabling informed risk management decisions.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle.	
SA-9	**EXTERNAL INFORMATION SYSTEM SERVICES**	Previous SEC 501-06 Control References: 4.3.2
	Control: The organization:	
a.	Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable laws, directives, policies, regulations, standards, and guidance;	
b.	Defines and documents government oversight and user roles and responsibilities with regard to external information system services; and	
c.	Monitors security control compliance by external service providers.	
	Supplemental Guidance: An external information system service is a service that is implemented outside of the authorization boundary of the organizational information system (i.e., a service that is used by, but not a part of, the organizational information system). Relationships with external service providers are established in a variety of ways, for example, through joint ventures, business partnerships, outsourcing arrangements (i.e., contracts, interagency agreements, lines of business arrangements), licensing agreements, and/or supply chain exchanges. The responsibility for adequately mitigating risks arising from the use of external information system services remains with the authorizing official. Authorizing officials require that an appropriate chain of trust be established with external service providers when dealing with the many issues associated with information security. For services external to the organization, a chain of trust requires that the organization establish and retain a level of confidence that each participating provider in the potentially complex consumer-provider relationship provides adequate protection for the services rendered to the organization. The extent and nature of this chain of trust varies based on the relationship between the organization and the external provider. Where a sufficient level of trust cannot be established in the external services and/or service providers, the organization employs compensating security controls or accepts the greater degree of risk. The external information system services documentation includes government, service provider, and end user security roles and responsibilities, and any service-level agreements. Service-level agreements define the expectations of performance for each required security control, describe measurable outcomes, and identify remedies and response requirements for any identified instance of noncompliance.	
	Control Enhancements for Sensitive Systems: None	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers. 12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess. 12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	
SA-10	**DEVELOPER CONFIGURATION MANAGEMENT**	Previous SEC 501-06 Control References: None
	Control: The organization requires that information system developers/integrators:	
a.	Perform configuration management during information system design, development, implementation, and operation;	
b.	Manage and control changes to the information system;	
c.	Implement only organization-approved changes;	
d.	Document approved changes to the information system; and	
e.	Track security flaws and flaw resolution.	
	Supplemental Guidance: Related controls: CM-3, CM-4, CM-9.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SA-11	**DEVELOPER SECURITY TESTING**	Previous SEC 501-06 Control References: 4.7.2
	Control: The organization requires that information system developers/integrators, in consultation with associated security personnel (including security engineers):	
a.	Create and implement a security test and evaluation plan;	
b.	Implement a verifiable flaw remediation process to correct weaknesses and deficiencies identified during the security testing and evaluation process; and	
c.	Document the results of the security testing/evaluation and flaw remediation processes.	
	Supplemental Guidance: Developmental security test results are used to the greatest extent feasible after verification of the results and recognizing that these results are impacted whenever there have been security-relevant modifications to the information system subsequent to developer testing. Test results may be used in support of the security authorization process for the delivered information system. Related control: CA-2, SI-2.	
	Control Enhancements for Sensitive Systems:	
(2)	The organization requires that information system developers/integrators perform a vulnerability analysis to document vulnerabilities, exploitation potential, and risk mitigations.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	
2.16	***FAMILY:*** *SYSTEM AND COMMUNICATIONS PROTECTION*	***CLASS:*** *TECHNICAL*
SC-2	**APPLICATION PARTITIONING**	Previous SEC 501-06 Control References: None
	Control: The information system separates user functionality (including user interface services) from information system management functionality.	
	Supplemental Guidance: Information system management functionality includes, for example, functions necessary to administer databases, network components, workstations, or servers, and typically requires privileged user access. The separation of user functionality from information system management functionality is either physical or logical and is accomplished by using different computers, different central processing units, different instances of the operating system, different network addresses, combinations of these methods, or other methods as appropriate. An example of this type of separation is observed in web administrative interfaces that use separate authentication methods for users of any other information system resources. This may include isolating the administrative interface on a different domain and with additional access controls.	
	DMV-Specific Requirements: Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators. PCI 8.5.16 VITA SC-2	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	
SC-3	**SECURITY FUNCTION ISOLATION**	Previous SEC 501-06 Control References: None
	Control: The information system isolates security functions from nonsecurity functions.	
	Supplemental Guidance: The information system isolates security functions from nonsecurity functions by means of an isolation boundary (implemented via partitions and domains) that controls access to and protects the integrity of, the hardware, software, and firmware that perform those security functions. The information system maintains a separate execution domain (e.g., address space) for each executing process. Related control: SA-13.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-4	**INFORMATION IN SHARED RESOURCES**	Previous SEC 501-06 Control References: None
	Control: The information system prevents unauthorized and unintended information transfer via shared system resources.	
	Supplemental Guidance: The purpose of this control is to prevent information, including encrypted representations of information, produced by the actions of a prior user/role (or the actions of a process acting on behalf of a prior user/role) from being available to any current user/role (or current process) that obtains access to a shared system resource (e.g., registers, main memory, secondary storage) after that resource has been released back to the information system. Control of information in shared resources is also referred to as object reuse. This control does not address: (i) information remanence which refers to residual representation of data that has been in some way nominally erased or removed; (ii) covert channels where shared resources are manipulated to achieve a violation of information flow restrictions; or (iii) components in the information system for which there is only a single user/role.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-5	**DENIAL OF SERVICE PROTECTION**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system protects against or limits the effects of denial of service attacks.	
	Supplemental Guidance: A variety of technologies exist to limit, or in some cases, eliminate the effects of denial of service attacks. For example, boundary protection devices can filter certain types of packets to protect devices on an organization's internal network from being directly affected by denial of service attacks. Employing increased capacity and bandwidth combined with service redundancy may reduce the susceptibility to some denial of service attacks. Related control: SC-7.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-7	**BOUNDARY PROTECTION**	Previous SEC 501-06 Control References: none
	Control: The information system:	
a.	Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
b.	Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.	
	Supplemental Guidance: Restricting external web traffic only to organizational web servers within managed interfaces and prohibiting external traffic that appears to be spoofing an internal address as the source are examples of restricting and prohibiting communications. Managed interfaces employing boundary protection devices include, for example, proxies, gateways, routers, firewalls, guards, or encrypted tunnels arranged in an effective security architecture (e.g., routers protecting firewalls and application gateways residing on a protected subnetwork commonly referred to as a demilitarized zone or DMZ). The organization considers the intrinsically shared nature of commercial telecommunications services in the implementation of security controls associated with the use of such services. Commercial telecommunications services are commonly based on network components and consolidated management systems shared by all attached commercial customers, and may include third-party provided access lines and other service elements. Consequently, such interconnecting transmission services may represent sources of increased risk despite contract security provisions. Therefore, when this situation occurs, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-4, IR-4, SC-5.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization physically allocates publicly accessible information system components to separate subnetworks with separate physical network interfaces.	
	Enhancement Supplemental Guidance: Publicly accessible information system components include, for example, public web servers.	
(2)	The information system prevents public access into the organization's internal networks except as appropriately mediated by managed interfaces employing boundary protection devices.	
(3)	The organization limits the number of access points to the information system to allow for more comprehensive monitoring of inbound and outbound communications and network traffic.	
	Enhancement Supplemental Guidance: The Trusted Internet Connection (TIC) initiative is an example of limiting the number of managed network access points.	
(4)	The organization:	
(a)	Implements a managed interface for each external telecommunication service;	
(b)	Establishes a traffic flow policy for each managed interface;	
(c)	Employs security controls as needed to protect the confidentiality and integrity of the information being transmitted;	
(d)	Documents each exception to the traffic flow policy with a supporting mission/business need and duration of that need;	
(e)	Reviews exceptions to the traffic flow policy once every 60-days at a minimum; and	
(f)	Removes traffic flow policy exceptions that are no longer supported by an explicit mission/business need.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(5)	The information system at managed interfaces, denies network traffic by default and allows network traffic by exception (i.e., deny all, permit by exception).	
(6)	The organization prevents the unauthorized release of information outside of the information system boundary or any unauthorized communication through the information system boundary when there is an operational failure of the boundary protection mechanisms.	
(7)	The information system prevents remote devices that have established a non-remote connection with the system from communicating outside of that communications path with resources in external networks.	
	Enhancement Supplemental Guidance: This control enhancement is implemented within the remote device (e.g., notebook/laptop computer) via configuration settings that are not configurable by the user of that device. An example of a non-remote communications path from a remote device is a virtual private network. When a non-remote connection is established using a virtual private network, the configuration settings prevent split-tunneling. Split tunneling might otherwise be used by remote users to communicate with the information system as an extension of that system and to communicate with local resources such as a printer or file server. Since the remote device, when connected by a non-remote connection, becomes an extension of the information system, allowing dual communications paths such as split-tunneling would be, in effect, allowing unauthorized external connections into the system.	
(12)	The information system implements host-based boundary protection mechanisms for servers, workstations, and mobile devices.	
	Enhancement Supplemental Guidance: A host-based boundary protection mechanism is, for example, a host-based firewall. Host-based boundary protection mechanisms are employed on mobile devices, such as notebook/laptop computers, and other types of mobile devices where such boundary protection mechanisms are available.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. 1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ. 1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ. 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications	
SC-8	**TRANSMISSION INTEGRITY**	Previous SEC 501-06 Control References: 4.7.2.4
	Control: The information system protects the integrity of transmitted information.	
	Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission integrity. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs cryptographic mechanisms to recognize changes to information during transmission unless otherwise protected by alternative physical measures.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. WEP is not permitted.	
SC-8-COV	**TRANSMISSION INTEGRITY (COV)**	Previous SEC 501-06 Control References: None
	Control: Require encryption or digital signatures for the transmission of email and attached data that is sensitive relative to integrity.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	
SC-9	**TRANSMISSION CONFIDENTIALITY**	Previous SEC 501-06 Control References: 4.7.2.4
	Control: The information system protects the confidentiality of transmitted information.	
	Supplemental Guidance: This control applies to communications across internal and external networks. If the organization is relying on a commercial service provider for transmission services as a commodity item rather than a fully dedicated service, it may be more difficult to obtain the necessary assurances regarding the implementation of needed security controls for transmission confidentiality. When it is infeasible or impractical to obtain the necessary security controls and assurances of control effectiveness through appropriate contracting vehicles, the organization either implements appropriate compensating security controls or explicitly accepts the additional risk. Related controls: AC-17, PE-4.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs cryptographic mechanisms to prevent unauthorized disclosure of information during transmission unless otherwise protected by organization-defined alternative physical measures.	
	Enhancement Supplemental Guidance: Alternative physical protection measures include, for example, protected distribution systems. Related control: SC-13.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. 4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. WEP is not permitted.	
SC-9-COV	**TRANSMISSION CONFIDENTIALITY (COV)**	Previous SEC 501-06 Control References: None
	Control: Require encryption for the transmission of email and attached data that is sensitive relative to confidentiality. The ISO should consider and plan for the issue of agency email being intercepted, incorrectly addressed, or infected with a virus.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	
SC-10	**NETWORK DISCONNECT**	Previous SEC 501-06 Control References: 5.4.2.7 Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system terminates the network connection associated with a communications session at the end of the session or after 30-minutes of inactivity.	
	Supplemental Guidance: This control applies to both internal and external networks. Terminating network connections associated with communications sessions include, for example, de-allocating associated TCP/IP address/port pairs at the operating-system level, or de-allocating networking assignments at the application level if multiple application sessions are using a single, operating system-level network connection. The time period of inactivity may, as the organization deems necessary, be a set of time periods by type of network access or for specific accesses.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.3.8 Automatic disconnect of sessions for remote access technologies after a specific period of inactivity.	
SC-12	**CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT**	Previous SEC 501-06 Control References: 6.3.2

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Control: The organization establishes and manages cryptographic keys for required cryptography employed within the information system.	
	Supplemental Guidance: Cryptographic key management and establishment can be performed using manual procedures or automated mechanisms with supporting manual procedures. In addition to being required for the effective operation of a cryptographic mechanism, effective cryptographic key management provides protections to maintain the availability of the information in the event of the loss of cryptographic keys by users.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization maintains availability of information in the event of the loss of cryptographic keys by users.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures 3.5 Protect any keys used to secure cardholder data against both disclosure and misuse. 3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary. 3.5.2 Store cryptographic keys securely in the fewest possible locations and forms. 3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following: 3.6.1 Generation of strong cryptographic keys. 3.6.2 Secure cryptographic key distribution. 3.6.3 Secure cryptographic key storage. 3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57). 3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. 3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction. 3.6.7 Prevention of unauthorized substitution of cryptographic keys. 3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	
SC-13	**USE OF CRYPTOGRAPHY**	Previous SEC 501-06 Control References: 6.3.2
	Control: The information system implements required cryptographic protections using cryptographic modules that comply with applicable laws, directives, policies, regulations, standards, and guidance.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems:	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. 6.5.3 Insecure cryptographic storage 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	
SC-14	**PUBLIC ACCESS PROTECTIONS**	Previous SEC 501-06 Control References: None
	Control: The information system protects the integrity and availability of publicly available information and applications.	
	Supplemental Guidance: The purpose of this control is to ensure that organizations explicitly address the protection needs for public information and applications with such protection likely being implemented as part of other security controls.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-17	**PUBLIC KEY INFRASTRUCTURE CERTIFICATES**	Previous SEC 501-06 Control References: None
	Control: The organization obtains public key certificates under an appropriate certificate policy from an approved service provider.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-20	**SECURE NAME / ADDRESS RESOLUTION SERVICE (AUTHORITATIVE SOURCE)**	Previous SEC 501-06 Control References: None
	Control: The information system provides additional data origin and integrity artifacts along with the authoritative data the system returns in response to name/address resolution queries.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: This control enables remote clients to obtain origin authentication and integrity verification assurances for the host/service name to network address resolution information obtained through the service. A domain name system (DNS) server is an example of an information system that provides name/address resolution service. Digital signatures and cryptographic keys are examples of additional artifacts. DNS resource records are examples of authoritative data.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SC-23	**SESSION AUTHENTICITY**	Previous SEC 501-06 Control References: None
	Control: The information system provides mechanisms to protect the authenticity of communications sessions.	
	Supplemental Guidance: This control focuses on communications protection at the session, versus packet, level. The intent of this control is to establish grounds for confidence at each end of a communications session in the ongoing identity of the other party and in the validity of the information being transmitted. For example, this control addresses man-in-the-middle attacks including session hijacking or insertion of false information into a session. This control is only implemented where deemed necessary by the organization (e.g., sessions in service-oriented architectures providing web-based services).	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only established connections are allowed into the network.)	
SC-28	**PROTECTION OF INFORMATION AT REST**	Previous SEC 501-06 Control References: None
	Control: The information system protects the confidentiality and integrity of information at rest.	
	Supplemental Guidance: This control is intended to address the confidentiality and integrity of information at rest in nonmobile devices and covers user information and system information. Information at rest refers to the state of information when it is located on a secondary storage device (e.g., disk drive, tape drive) within an organizational information system. Configurations and/or rule sets for firewalls, gateways, intrusion detection/prevention systems, and filtering routers and authenticator content are examples of system information likely requiring protection. Organizations may choose to employ different mechanisms to achieve confidentiality and integrity protections, as appropriate.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization employs cryptographic mechanisms to prevent unauthorized disclosure and modification of information at rest unless otherwise protected by alternative physical measures.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	DMV-Specific Requirements: To address PCI 1.2.2 - 1. This is a recommended process; a file integrity tool would achieve the same results, as would other feasible processes. Whichever approach is used must be functionally equivalent a. Export firewall configuration files after any network configuration change b. Extract configuration files to a secure backup device c. Calculate a Message Digest 5 (MD5) hash for each configuration file and save this calculated hash to a separate location d. Prior to loading any configuration file, calculate its MD5 hash and compare to its corresponding hash from item b. above – they should match exactly	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 1.2.2 Secure and synchronize router configuration files. 1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	
2.17	***FAMILY:*** *SYSTEM AND INFORMATION INTEGRITY*	***CLASS:*** *OPERATIONAL*
SI-2	**FLAW REMEDIATION**	Previous SEC 501-06 Control References: 4.7.2.14
	Control: The organization:	
a.	Identifies, reports, and corrects information system flaws;	
b.	Tests software updates related to flaw remediation for effectiveness and potential side effects on organizational information systems before installation; and	
c	Incorporates flaw remediation into the organizational configuration management process.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The organization identifies information systems containing software affected by recently announced software flaws (and potential vulnerabilities resulting from those flaws) and reports this information to designated organizational officials with information security responsibilities (e.g., senior information security officers, information system security managers, information systems security officers). The organization (including any contractor to the organization) promptly installs security-relevant software updates (e.g., patches, service packs, and hot fixes). Flaws discovered during security assessments, continuous monitoring, incident response activities, or information system error handling, are also addressed expeditiously. Organizations are encouraged to use resources such as the Common Weakness Enumeration (CWE) or Common Vulnerabilities and Exposures (CVE) databases in remediating flaws discovered in organizational information systems. By requiring that flaw remediation be incorporated into the organizational configuration management process, it is the intent of this control that required/anticipated remediation actions are tracked and verified. An example of expected flaw remediation that would be so verified is whether the procedures contained in US Special CERT guidance and Information Assurance Vulnerability Alerts have been accomplished. Related controls: CA-2, CA-7, CM-3, MA-2, IR-4, RA-5, SA-11, SI-11.	
	DMV-Specific Requirements: 1. All security patches/updates rated "Critical" by their vendor must be installed in the production environment within 30 days of their release 2. All other required patches must be installed in the production environment within 90 days of their release PCI 6.1 VITA SI-2	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release. 6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	
SI-2-COV	**FLAW REMEDIATION (COV)**	Previous SEC 501-06 Control References: 4.7.2.14
	Control: The organization:	
1	Apply all software publisher security updates to the associated software products.	
2	All security updates must be applied as soon as possible after appropriate testing, not to exceed 90 days for implementation.	
3	Prohibit the use of software products that the software publisher has designated as End-of-Life (i.e. software publisher no longer provides security patches for the software product).	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
SI-3	**MALICIOUS CODE PROTECTION**	Previous SEC 501-06 Control References: 4.5
	Control: The organization:	
a.	Employs malicious code protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and eradicate malicious code:	
	Transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; or	
	Inserted through the exploitation of information system vulnerabilities;	
b.	Updates malicious code protection mechanisms (including signature definitions) whenever new releases are available in accordance with organizational configuration management policy and procedures;	
c.	Configures malicious code protection mechanisms to:	
	Perform periodic scans of the information system once a week and real-time scans of files from external sources as the files are downloaded, opened, or executed in accordance with organizational security policy; and	
	quarantine malicious code; send alert to administrator; in response to malicious code detection; and	
d.	Addresses the receipt of false positives during malicious code detection and eradication and the resulting potential impact on the availability of the information system.	
	Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Malicious code includes, for example, viruses, worms, Trojan horses, and spyware. Malicious code can also be encoded in various formats (e.g., UUENCODE, Unicode) or contained within a compressed file. Removable media includes, for example, USB devices, diskettes, or compact disks. A variety of technologies and methods exist to limit or eliminate the effects of malicious code attacks. Pervasive configuration management and strong software integrity controls may be effective in preventing execution of unauthorized code. In addition to commercial off-the-shelf software, malicious code may also be present in custom-built software. This could include, for example, logic bombs, back doors, and other types of cyber attacks that could affect organizational missions and business functions. Traditional malicious code protection mechanisms are not built to detect such code. In these situations, organizations must rely instead on other risk mitigation measures to include, for example, secure coding practices, trusted procurement processes, configuration management and control, and monitoring practices to help ensure that software does not perform functions other than those intended. Related controls: SA-4, SA-8, SA-12, SA-13, SI-4, SI-7.	
	Control Enhancements for Sensitive Systems:	
(1)	The organization centrally manages malicious code protection mechanisms.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
(2)	The information system automatically updates malicious code protection mechanisms (including signature definitions).	
(3)	The information system prevents non-privileged users from circumventing malicious code protection capabilities.	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	
SI-3-COV	**MALICIOUS CODE PROTECTION (COV)**	Previous SEC 501-06 Control References: 4.5.2
	Control: 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.).	
2	Prohibit all IT system users from knowingly propagating malicious programs including opening attachments from unknown sources.	
3	Provide malicious code protection mechanisms via multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.	
4	Provide protection against malicious program through the use of mechanisms 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.	
5	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.	
6	Require all forms of malicious code protection to start automatically upon system boot.	
7	Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
8	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.	
9	Require use of only new media (e.g. diskettes, CD-ROM) or sanitized media for making copies of software for distribution.	
10	Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.	
11	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.	
12	Establish Operating System (OS) update schedules commensurate with sensitivity and risk.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	
SI-4	**INFORMATION SYSTEM MONITORING**	Previous SEC 501-06 Control References: 9.2.2/9.3.2
	Control: The organization:	
a.	Monitors events on the information system and detects information system attacks;	
b.	Identifies unauthorized use of the information system;	
d.	Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Commonwealth based on law enforcement information, intelligence information, or other credible sources of information; and	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Information system monitoring includes external and internal monitoring. External monitoring includes the observation of events occurring at the system boundary (i.e., part of perimeter defense and boundary protection). Internal monitoring includes the observation of events occurring within the system (e.g., within internal organizational networks and system components). Information system monitoring capability is achieved through a variety of tools and techniques (e.g., intrusion detection systems, intrusion prevention systems, malicious code protection software, audit record monitoring software, network monitoring software). Strategic locations for monitoring devices include, for example, at selected perimeter locations and near server farms supporting critical applications, with such devices typically being employed at the managed interfaces associated with controls SC-7 and AC-17. The Einstein network monitoring device from the Department of Homeland Security is an example of a system monitoring device. The granularity of the information collected is determined by the organization based on its monitoring objectives and the capability of the information system to support such activities. An example of a specific type of transaction of interest to the organization with regard to monitoring is Hyper Text Transfer Protocol (HTTP) traffic that bypasses organizational HTTP proxies, when use of such proxies is required. Related controls: AC-4, AC-8, AC-17, AU-2, AU-6, SI-3, SI-7.	
	Control Enhancements for Sensitive Systems:	
(4)	The information system monitors inbound and outbound communications for unusual or unauthorized activities or conditions.	
	Enhancement Supplemental Guidance: Unusual/unauthorized activities or conditions include, for example, internal traffic that indicates the presence of malicious code within an information system or propagating among system components, the unauthorized export of information, or signaling to an external information system. Evidence of malicious code is used to identify potentially compromised information systems or information system components.	
(6)	The information system prevents non-privileged users from circumventing intrusion detection and prevention capabilities.	
(14)	The organization employs a wireless intrusion detection system to identify rogue wireless devices and to detect attack attempts and potential compromises/breaches to the information system.	
(15)	The organization employs an intrusion detection system to monitor wireless communications traffic as the traffic passes from wireless to wireline networks.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers). 5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software. 5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs. 11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date. 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.5.5 Monitor and control all access to data.	
SI-5	**SECURITY ALERTS, ADVISORIES, AND DIRECTIVES**	Previous SEC 501-06 Control References: None
	Control: The organization:	
a.	Receives information system security alerts, advisories, and directives from designated external organizations on an ongoing basis;	
b.	Generates internal security alerts, advisories, and directives as deemed necessary;	
c.	Disseminates security alerts, advisories, and directives to Management and/or IT Managers and/or DMV employees as appropriate; and	
d.	Implements security directives in accordance with established time frames, or notifies the issuing organization of the degree of noncompliance.	
	Supplemental Guidance: None	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel. 12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	
SI-7	**SOFTWARE AND INFORMATION INTEGRITY**	Previous SEC 501-06 Control References: 4.7.2.5-10 Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system detects unauthorized changes to software and information.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The organization employs integrity verification applications on the information system to look for evidence of information tampering, errors, and omissions. The organization employs good software engineering practices with regard to commercial off-the-shelf integrity mechanisms (e.g., parity checks, cyclical redundancy checks, cryptographic hashes) and uses tools to automatically monitor the integrity of the information system and the applications it hosts.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: 10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert). 11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly. **NOTE:** The requirement for weekly file comparisons (PCI 11.5) applies only to systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only. Control SI-7's requirements apply to all other DMV systems.	
SI-8	**SPAM PROTECTION**	Previous SEC 501-06 Control References: 4.5
	Control: The organization:	
a.	Employs spam protection mechanisms at information system entry and exit points and at workstations, servers, or mobile computing devices on the network to detect and take action on unsolicited messages transported by electronic mail, electronic mail attachments, web accesses, or other common means; and	
b.	Updates spam protection mechanisms (including signature definitions) when new releases are available in accordance with organizational configuration management policy and procedures.	
	Supplemental Guidance: Information system entry and exit points include, for example, firewalls, electronic mail servers, web servers, proxy servers, and remote-access servers. Related controls: SC-5, SI-3.	
	Control Enhancements for Sensitive Systems: None	
(1)	The organization centrally manages spam protection mechanisms.	
	PCI compliance: PCI-DSS has no requirement for this control.	
SI-9	**INFORMATION INPUT RESTRICTIONS**	Previous SEC 501-06 Control References: 5.2.2.1
	Control: The organization restricts the capability to input information to the information system to authorized personnel.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: Restrictions on organizational personnel authorized to input information to the information system may extend beyond the typical access controls employed by the system and include limitations based on specific operational/project responsibilities. Related controls: AC-5, AC-6.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: PCI-DSS has no requirement for this control.	
SI-10	**INFORMATION INPUT VALIDATION**	Previous SEC 501-06 Control References: 4.7.2.8
	Control: The information system checks the validity of information inputs.	
	Supplemental Guidance: Rules for checking the valid syntax and semantics of information system inputs (e.g., character set, length, numerical range, acceptable values) are in place to verify that inputs match specified definitions for format and content. Inputs passed to interpreters are prescreened to prevent the content from being unintentionally interpreted as commands.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: 6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XpPath injection flaws as well as other injection flaws. 6.5.2 Buffer overflow.	
SI-11	**ERROR HANDLING**	Previous SEC 501-06 Control References: None Withdrawn from SEC501-07 PORTIONS KEPT FOR DMV
	Control: The information system:	
a.	Identifies potentially security-relevant error conditions;	
b.	Generates error messages that provide information necessary for corrective actions without revealing sensitive or potentially harmful information in error logs and administrative messages that could be exploited by adversaries (i.e., prevents information leakage); and	
c.	Reveals error messages only to authorized personnel.	

No.	Control Family / Control Name / Guidance	Control Class / Prior References
	Supplemental Guidance: The structure and content of error messages are carefully considered by the organization. The extent to which the information system is able to identify and handle error conditions is guided by organizational policy and operational requirements. Sensitive information includes, for example, account numbers, social security numbers, and credit card numbers.	
	Control Enhancements for Sensitive Systems: None	
	PCI compliance: The requirements specified in this security control meet the following PCI-DSS requirements: 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: 6.5.5 Improper error handling.	

PCI-DSS 2.0 Requirements Not Addressed by VITA SEC501-07

The following PCI requirements do not have corresponding controls in VITA SEC501-07; these requirements apply only to DMV systems in-scope for PCI; those storing, processing or transmitting cardholder or transaction data only.		
No.	**PCI Requirement Group / Guidance**	**Comments**
3	***Protect stored cardholder data***	
3.2	Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3. Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.	
3.2.1	Do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	
3.2.2	Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	
3.2.3	Do not store the personal identification number (PIN) or the encrypted PIN block.	
3.3	Mask Primary Account Number (PAN) when displayed (the first six and last four digits are the maximum number of digits to be displayed).	
6	***Develop and maintain secure systems and applications***	
	Supplemental Guidance: (PCI 6.3) Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging), and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	
6.3.1	Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.	
	Supplemental Guidance: (PCI 6.4) Follow change control processes and procedures for all changes to system components. The processes must include the following:	
6.4.4	Removal of test data and accounts before production systems become active.	

No.	PCI Requirement Group / Guidance	Comments
6.4.5.4	Back-out procedures.	
	Supplemental Guidance: (PCI 6.2) Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. Notes: Risk rankings should be based on industry best practices. For example, criteria for ranking High risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as Critical, and/or a vulnerability affecting a critical system component.	
	Supplemental Guidance: (PCI 6.5) Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes (examples follow in 6.5.6-6.5.9). As industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the THEN current best practices must be used for these requirements.	
6.5.6	All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	SI-2 FLAW REMEDIATION recommends use of resources such as CWE / CVE databases in identifying software flaws but does not require ranking them according to risk
	Supplemental Guidance: Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external).	
6.5.7	Cross-site scripting (XSS).	
6.5.8	Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).	
6.5.9	Cross-site request forgery (CRSF).	
7	***Restrict access to cardholder data by business need to know***	
	Supplemental Guidance: (PCI 7.1) Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include:	
7.1.4	Implementation of an automated access control system.	

No.	PCI Requirement Group / Guidance	Comments
	Supplemental Guidance: (PCI 7.2) Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to —deny all‖ unless specifically allowed. This access control system must include the following:	
7.2.1	Coverage of all system components.	
9	***Restrict physical access to cardholder data***	
9.1.2	Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is specifically authorized.	
	Supplemental Guidance: Maintain strict control over the internal or external distribution of any kind of media (digital or non-digital) that contains cardholder or related data.	
9.8	Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	
9.9.1	Properly maintain inventory logs of all media and conduct media inventories at least annually.	
10	***Track and monitor all access to network resources and cardholder data***	
	Supplemental Guidance: (PCI 10.2) Implement automated audit trails for all system components to reconstruct the following events (items 10.2.3-10.2.7):	
10.2.3	Access to all audit trails.	
10.2.5	Use of identification and authentication mechanisms.	
10.2.6	Initialization of the audit logs.	
10.2.7	Creation and deletion of system-level objects.	
11	***Regularly test security systems and processes***	
11.2.2	Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	RA-5 and RA-5-COV VULNERABILITY SCANNING require vulnerability scans every 90 days but do not require ASVs perform them

No.	PCI Requirement Group / Guidance	Comments
11.2.3	Perform internal and external scans after any significant change.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV) requires post-change scans for Internet-facing sensitive system: "3.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."
	Supplemental Guidance: (PCI 11.3.1 Test) Network-layer penetration tests should include components that support network functions as well as operating systems. (PCI 11.3.2 Test) Application-layer penetration tests should include, at a minimum, the vulnerabilities listed in Requirement 6.5 (see section 6, **Supplemental Guidance (PCI 6.5)** above).	
11.3.1	Network-layer penetration tests.	
11.3.2	Application-layer penetration tests.	
12	***Maintain a policy that addresses information security for all personnel***	
	Supplemental Guidance: (PCI 12.3) Develop usage policies for critical technologies (for example, remote-access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), e-mail usage and Internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	
12.3.3	A list of all such devices and personnel with access	CM-2-COV BASELINE CONFIGURATION (COV) & CM-8 INFORMATION SYSTEM COMPONENT INVENTORY require inventory of devices but there is no requirement for identifying personnel with access
12.3.4	Labeling of devices to determine owner, contact information, and purpose.	VITA SEC501-07 has no requirement for asset tags, but they are used in practice to identify device owner, contact information and location.
12.3.7	List of company-approved products.	
12.3.9	Activation of remote access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	

No.	PCI Requirement Group / Guidance	Comments
12.3.10	For personnel accessing cardholder data via remote access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	

PCI DSS Requirements Version 2.0 to VITA SEC501-07 Cross-Reference		
PCI Requirements	**VITA/NIST Controls**	**VITA / NIST Control Family**
Requirement 1: Install and maintain a firewall configuration to protect cardholder data		
1.1 Establish firewall and router configuration standards that include the following:	No requirement specified	
1.1.1 A formal process for approving and testing all network connections and changes to the firewall and router configurations	CM-1 CONFIGURATION MANAGEMENT POLICY AND PROCEDURES CM-3 CONFIGURATION CHANGE CONTROL CM-9 CONFIGURATION MANAGEMENT PLAN	CM
1.1.2 Current network diagram with all connections to cardholder data, including any wireless networks.	CM-2 BASELINE CONFIGURATION	CM
1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.1.4 Description of groups, roles, and responsibilities for logical management of network components.	AC-5 SEPARATION OF DUTIES AC-6 LEAST PRIVILEGE	AC
1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure.	CM-6 CONFIGURATION SETTINGS CM-7 LEAST FUNCTIONALITY	CM
1.1.6 Requirement to review firewall and router rule sets at least every six months.	CM-2 BASELINE CONFIGURATION CM-2-COV BASELINE CONFIGURATION	CM
1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment.	SC-1 SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES SC-7 BOUNDARY PROTECTION	SC
1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment.	SC-7 BOUNDARY PROTECTION	SC
1.2.2 Secure and synchronize router configuration files.	SC-28 PROTECTION OF INFORMATION AT REST	SC
1.2.3 Install perimeter firewalls between any wireless networks and the cardholder data environment, and configure these firewalls to deny or control (if such traffic is necessary for business purposes) any traffic from the wireless environment into the cardholder data environment.	AC-4 INFORMATION FLOW ENFORCEMENT AC-18 WIRELESS ACCESS AC-18-COV WIRELESS ACCESS (COV)	AC
1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC
1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet.	AC-4 INFORMATION FLOW ENFORCEMENT SC-7 BOUNDARY PROTECTION	AC, SC

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
1.3.6 Implement stateful inspection, also known as dynamic packet filtering. (That is, only ”established” connections are allowed into the network.)	AC-4 INFORMATION FLOW ENFORCEMENT SC-23 SESSION AUTHENTICITY	AC, SC
1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks.	SC-7 BOUNDARY PROTECTION	SC
1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties.	SC-28 PROTECTION OF INFORMATION AT REST	SC
1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization’s network.	AC-19 ACCESS CONTROL FOR MOBILE DEVICES CM-7 LEAST FUNCTIONALITY SC-7 BOUNDARY PROTECTION	AC, CM, SC
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters		
2.1 Always change vendor-supplied defaults before installing a system on the network—including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	IA-5 AUTHENTICATOR MANAGEMENT	IA
2.1.1 For wireless environments connected to the cardholder data environment or transmitting cardholder data, change wireless vendor defaults, including but not limited to default wireless encryption keys, passwords, and SNMP community strings.	AC-4 INFORMATION FLOW ENFORCEMENT AC-18 WIRELESS ACCESS AC-18-COV WIRELESS ACCESS (COV)	AC
2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards.	CM-6 CONFIGURATION SETTINGS CM-7 LEAST FUNCTIONALITY	CM
2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) Note: Where virtualization technologies are in use, implement only one primary function per virtual system component.	CM-7 LEAST FUNCTIONALITY	CM
2.2.2 Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. Implement security features for any required services, protocols or daemons that are considered to be insecure.	CM-6 CONFIGURATION SETTINGS CM-7 LEAST FUNCTIONALITY	CM
2.2.3 Configure system security parameters to prevent misuse	AC-6 LEAST PRIVILEGE CM-6 CONFIGURATION SETTINGS	AC, CM
2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.	CM-6 CONFIGURATION SETTINGS CM-7 LEAST FUNCTIONALITY	CM
2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access.	AC-17 REMOTE ACCESS	AC
Requirement 3: Protect stored cardholder data		
3.1 Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes as follows:	No requirement specified	

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
3.1.1 Implement a data retention and disposal policy that includes: § Limiting data storage amount and retention time to that which is required for legal, regulatory, and business requirements. § Processes for secure deletion of data when no longer needed. § Specific retention requirements for cardholder data. § A quarterly automatic or manual process for identifying and securely deleting stored cardholder data that exceeds defined retention requirements.	SA-3-COV-1 LIFE CYCLE SUPPORT (COV) (Retention/sanitizing media)	SA
3.2 Do not store sensitive authentication data after authorization (even if encrypted). Sensitive authentication data includes the data as cited in the following Requirements 3.2.1 through 3.2.3. Note: It is permissible for issuers and companies that support issuing services to store sensitive authentication data if there is a business justification and the data is stored securely.	N/A	
3.2.1 Do not store the full contents of any track from the magnetic stripe (located on the back of a card, equivalent data contained on a chip, or elsewhere). This data is alternatively called full track, track, track 1, track 2, and magnetic-stripe data.	N/A	
3.2.2 Do not store the card-verification code or value (three-digit or four-digit number printed on the front or back of a payment card) used to verify card-not-present transactions.	N/A	
3.2.3 Do not store the personal identification number (PIN) or the encrypted PIN block.	N/A	
3.3 Mask PAN when displayed (the first six and last four digits are the maximum number of digits to be displayed).	N/A	
3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures Note: It is a relatively trivial effort for a malicious individual to reconstruct original PAN data if they have access to both the truncated and hashed version of a PAN. Where hashed and truncated versions of the same PAN are present in an entity's environment, additional controls should be in place to ensure that the hashed and truncated versions cannot be correlated to reconstruct the original PAN.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT SC-13 USE OF CRYPTOGRAPHY SC-28 PROTECTION OF INFORMATION AT REST	SC
3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts.	SC-13 USE OF CRYPTOGRAPHY SC-28 PROTECTION OF INFORMATION AT REST	SC
3.5 Protect any keys used to secure cardholder data against both disclosure and misuse: Note: This requirement also applies to key encryption keys used to protect data encrypting keys -- such key encryption keys must be at least as strong as the data encrypting key.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.5.1 Restrict access to cryptographic keys to the fewest number of custodians necessary.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.5.2 Store cryptographic keys securely in the fewest possible locations and forms.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6 Fully document and implement all key management processes and procedures for cryptographic keys used for encryption of cardholder data, including the following	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.1 Generation of strong cryptographic keys.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.2 Secure cryptographic key distribution.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.3 Secure cryptographic key storage.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
3.6.4 Cryptographic key changes for keys that have reached the end of their cryptoperiod (for example, after a defined period of time has passed and/or after a certain amount of cipher-text has been produced by a given key), as defined by the associated application vendor or key owner, and based on industry best practices and guidelines (for example, NIST Special Publication 800-57).	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.5 Retirement or replacement (for example, archiving, destruction, and/or revocation) of keys as deemed necessary when the integrity of the key has been weakened (for example, departure of an employee with knowledge of a clear-text key), or keys are suspected of being compromised. Note: If retired or replaced cryptographic keys need to be retained, these keys must be securely archived (for example, by using a key encryption key). Archived cryptographic keys should only be used for decryption/verification purposes.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.6 If manual clear-text cryptographic key management operations are used, these operations must be managed using split knowledge and dual control (for example, requiring two or three people, each knowing only their own key component, to reconstruct the whole key). Note: Examples of manual key management operations include, but are not limited to: key generation, transmission, loading, storage and destruction.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.7 Prevention of unauthorized substitution of cryptographic keys.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
3.6.8 Requirement for cryptographic key custodians to formally acknowledge that they understand and accept their key-custodian responsibilities.	SC-12 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT	SC
Requirement 4: Encrypt transmission of cardholder data across open, public networks		
4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks.	AC-17 REMOTE ACCESS (addresses remote sessions for sensitive systems) AC-17-COV REMOTE ACCESS (COV) SC-8 TRANSMISSION INTEGRITY SC-9 TRANSMISSION CONFIDENTIALITY	AC, SC
4.1.1 Ensure wireless networks transmitting cardholder data or connected to the cardholder data environment, use industry best practices (e.g., IEEE 802.11i) to implement strong encryption for authentication and transmission. Note: The use of WEP as a security control was prohibited as of 30 June, 2010.	AC-18 WIRELESS ACCESS AC-18-COV WIRELESS ACCESS (COV) SC-8 TRANSMISSION INTEGRITY SC-9 TRANSMISSION CONFIDENTIALITY	AC, SC
4.2 Never send unprotected PANs by end-user messaging technologies (for example, e-mail, instant messaging, chat, etc.).	SC-8-COV TRANSMISSION INTEGRITY (COV) SC-9-COV TRANSMISSION CONFIDENTIALITY (COV)	SC
Requirement 5: Use and regularly update anti-virus software or programs		
5.1 Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	AC-19 ACCESS CONTROL FOR MOBILE DEVICES SI-3 MALICIOUS CODE PROTECTION SI-3-COV MALICIOUS CODE PROTECTION (COV) SI-4 INFORMATION SYSTEM MONITORING	AC, SI
5.1.1 Ensure that all anti-virus programs are capable of detecting, removing, and protecting against all known types of malicious software.	AC-19 ACCESS CONTROL FOR MOBILE DEVICES SI-3 MALICIOUS CODE PROTECTION SI-3-COV MALICIOUS CODE PROTECTION (COV) SI-4 INFORMATION SYSTEM MONITORING	AC, SI

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
5.2 Ensure that all anti-virus mechanisms are current, actively running, and generating audit logs.	AC-19 ACCESS CONTROL FOR MOBILE DEVICES SI-3 MALICIOUS CODE PROTECTION SI-3-COV MALICIOUS CODE PROTECTION (COV) SI-4 INFORMATION SYSTEM MONITORING	AC, SI
Requirement 6: Develop and maintain secure systems and applications		
6.1 Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed. Install critical security patches within one month of release.	SI-2 FLAW REMEDIATION SI-2-COV FLAW REMEDIATION (COV)	SI
6.2 Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities. **Note:** Risk rankings should be based on industry best practices. For example, criteria for ranking "High" risk vulnerabilities may include a CVSS base score of 4.0 or above, and/or a vendor-supplied patch classified by the vendor as "critical," and/or a vulnerability affecting a critical system component.	RA-5 VULNERABILITY SCANNING SI-2 FLAW REMEDIATION	RA, SI
6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. These processes must include the following:	SA-3 LIFE CYCLE SUPPORT SA-3-COV-1 LIFE CYCLE SUPPORT (COV) SA-3-COV-2 LIFE CYCLE SUPPORT (COV) SA-8 SECURITY ENGINEERING PRINCIPLES	SA
6.3.1 Removal of custom application accounts, user IDs, and passwords before applications become active or are released to customers.	N/A	
6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. **Note:** This requirement for code reviews applies to all custom code (both internal and public-facing), as part of the system development lifecycle. Code reviews can be conducted by knowledgeable internal personnel or third parties. Web applications are also subject to additional controls, if they are public facing, to address ongoing threats and vulnerabilities after implementation, as defined at PCI DSS Requirement 6.6.	RA-5 VULNERABILITY SCANNING SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	RA, SA
6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following:	SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	SA
6.4.1 Separate development/test and production environments.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	SA
6.4.2 Separation of duties between development/test and production environments.	AC-5 SEPARATION OF DUTIES SA-3 LIFE CYCLE SUPPORT	AC, SA
6.4.3 Production data (live PANs) are not used for testing or development.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	SA
6.4.4 Removal of test data and accounts before production systems become active.	N/A	
6.4.5 Change control procedures for the implementation of security patches and software modifications. Procedures must include the following:	CM-3 CONFIGURATION CHANGE CONTROL CM-3-COV CONFIGURATION CHANGE CONTROL (COV) CM-9 CONFIGURATION MANAGEMENT PLAN	CM

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
6.4.5.1 Documentation of impact.	CA-7 CONTINUOUS MONITORING CM-3 CONFIGURATION CHANGE CONTROL CM-4 SECURITY IMPACT ANALYSIS	CA, CM
6.4.5.2 Documented change approval by authorized parties.	CM-3 CONFIGURATION CHANGE CONTROL	CM
6.4.5.3 Functionality testing to verify that the change does not adversely impact the security of the system.	CA-7 CONTINUOUS MONITORING CM-3-COV CONFIGURATION CHANGE CONTROL (COV) CM-4 SECURITY IMPACT ANALYSIS SA-11 DEVELOPER SECURITY TESTING	CA, CM, SA
6.4.5.4 Back-out procedures.	N/A	
6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: **Note:** The vulnerabilities listed at 6.5.1 through 6.5.9 were current with industry best practices when this version of PCI DSS was published. However, as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.	SA-3 LIFE CYCLE SUPPORT SA-3-COV-1 LIFE CYCLE SUPPORT (COV) SA-3-COV-2 LIFE CYCLE SUPPORT (COV) SI-10 INFORMATION INPUT VALIDATION SI-11 ERROR HANDLING	SA, SI
6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XpPath injection flaws as well as other injection flaws.	SI-10 INFORMATION INPUT VALIDATION	
6.5.2 Buffer overflow.	SI-10 INFORMATION INPUT VALIDATION	
6.5.3 Insecure cryptographic storage	IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION SC-13 USE OF CRYPTOGRAPHY	IA, SC
6.5.4 Insecure communications.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	SA
6.5.5 Improper error handling.	SI-11 ERROR HANDLING	SI
6.5.6 All "High" vulnerabilities identified in the vulnerability identification process (as defined in PCI DSS Requirement 6.2).	SI-2 FLAW REMEDIATION recommends use of resources such as CWE / CVE databases in identifying software flaws but does not require ranking them according to risk	SI
Requirements 6.5.7 through 6.5.9, below, apply to web applications and application interfaces (internal or external): **6.5.7** Cross-site scripting (XSS).	N/A	
6.5.8 Improper Access Control (such as insecure direct object references, failure to restrict URL access, and directory traversal).	N/A	
6.5.9 Cross-site request forgery (CRSF).	N/A	
6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications	RA-5 VULNERABILITY SCANNING RA-5-COV VULNERABILITY SCANNING (COV) SC-7 BOUNDARY PROTECTION	RA, SC
Requirement 7: Restrict access to cardholder data by business need to know		

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
7.1 Limit access to system components and cardholder data to only those individuals whose job requires such access. Access limitations must include the following:	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE	AC
7.1.1 Restriction of access rights to privileged user IDs to least privileges necessary to perform job responsibilities	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE	AC
7.1.2 Assignment of privileges is based on individual personnel's job classification and function	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE PS-2 POSITION CATEGORIZATION	AC
7.1.3 Requirement for a documented approval by authorized parties specifying required privileges.	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE	AC
7.1.4 Implementation of an automated access control system.	N/A	
7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. This access control system must include the following:	AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	AC
7.2.1 Coverage of all system components.	N/A	
7.2.2 Assignment of privileges to individuals based on job classification and function.	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV) AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE	AC
7.2.3 Default "deny-all" setting.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV)	SA
Requirement 8: Assign a unique ID to each person with computer access		
8.1 Assign all users a unique username before allowing them to access system components or cardholder data.	IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) IA-4 IDENTIFIER MANAGEMENT	IA
8.2 In addition to assigning a unique ID**,** employ at least one of the following methods to authenticate all users: § Something you know, such as a password or passphrase § Something you have, such as a token device or smart card § Something you are, such as a biometric	IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)	IA

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) Note: Two-factor authentication requires that two of the three authentication methods (see Req. 8.2 for descriptions of authentication methods) be used for authentication. Using one factor twice (e.g. using two separate passwords) is not considered two-factor authentication.	AC-17 REMOTE ACCESS	AC
8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.	IA-5 AUTHENTICATOR MANAGEMENT SC-13 USE OF CRYPTOGRAPHY SC-28 PROTECTION OF INFORMATION AT REST	IA, SC
8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows:	AC-2 ACCOUNT MANAGEMENT IA-4 IDENTIFIER MANAGEMENT IA-5 AUTHENTICATOR MANAGEMENT RA-2 SECURITY CATEGORIZATION	AC, IA, PS
8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects.	AC-2 ACCOUNT MANAGEMENT IA-4 IDENTIFIER MANAGEMENT	AC, IA
8.5.2 Verify user identity before performing password resets	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.3 Set passwords for first-time use and resets to a unique value for each user and change immediately after the first use.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.4 Immediately revoke access for any terminated users.	IA-5 AUTHENTICATOR MANAGEMENT PS-4 PERSONNEL TERMINATION	IA
8.5.5 Remove/disable inactive user accounts at least every 90 days.	AC-2 ACCOUNT MANAGEMENT IA-4 IDENTIFIER MANAGEMENT	AC, IA
8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.	AC-17 REMOTE ACCESS	AC
8.5.7 Communicate authentication procedures and policies to all users who have access to cardholder data.	AT-2 SECURITY AWARENESS AT-2-COV SECURITY AWARENESS (COV) PL-4 RULES OF BEHAVIOR PS-6 ACCESS AGREEMENTS	AT, PL, PS
8.5.8 Do not use group, shared, or generic accounts and passwords, or other authentication methods.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.9 Change user passwords at least every 90 days.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.10 Require a minimum password length of at least seven characters.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.11 Use passwords containing both numeric and alphabetic characters.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.12 Do not allow an individual to submit a new password that is the same as any of the last four passwords he or she has used.	IA-5 AUTHENTICATOR MANAGEMENT	IA
8.5.13 Limit repeated access attempts by locking out the user ID after not more than six attempts.	AC-7 UNSUCCESSFUL LOGIN ATTEMPTS	AC

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
8.5.14 Set the lockout duration to a minimum of 30 minutes or until administrator enables the user ID.	AC-7 UNSUCCESSFUL LOGIN ATTEMPTS	AC
8.5.15 If a session has been idle for more than 15 minutes, require the user to re-authenticate to re-activate the terminal or session.	AC-11 SESSION LOCK	AC
8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.	SC-2 APPLICATION PARTITIONING (Generally mentions separating user from adminstrative functionality - does not address this specifically)	SC
Requirement 9: Restrict physical access to cardholder data		
9.1 Use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment.	PE-2 PHYSICAL ACCESS AUTHORIZATIONS PE-3 PHYSICAL ACCESS CONTROL PE-5 ACCESS CONTROL FOR OUTPUT DEVICES PE-6 MONITORING PHYSICAL ACCESS	PE
9.1.1 Use video cameras and/or access control mechanisms to monitor individual physical access to sensitive areas. Review collected data and correlate with other entries. Store for at least three months, unless otherwise restricted by law.	PE-6 MONITORING PHYSICAL ACCESS (Review access logs every 60 days)	PE
9.1.2 Restrict physical access to publicly accessible network jacks. For example, areas accessible to visitors should not have network ports enabled unless network access is specifically authorized.	N/A	
9.1.3 Restrict physical access to wireless access points, gateways, handheld devices, networking/communications hardware, and telecommunications lines.	PE-3 PHYSICAL ACCESS CONTROL PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM	PE
9.2 Develop procedures to easily distinguish between onsite personnel and visitors, especially in areas where cardholder data is accessible.	PE-7 VISITOR CONTROL PE-8 ACCESS RECORDS	PE
9.3 Make sure all visitors are handled as follows:	PE-7 VISITOR CONTROL	PE
9.3.1 Authorized before entering areas where cardholder data is processed or maintained.	PE-7 VISITOR CONTROL	PE
9.3.2 Given a physical token (for example, a badge or access device) that expires and that identifies the visitors as not onsite personnel.	PE-7 VISITOR CONTROL	PE
9.3.3 Asked to surrender the physical token before leaving the facility or at the date of expiration	PE-7 VISITOR CONTROL	PE
9.4 Use a visitor log to maintain a physical audit trail of visitor activity. Document the visitor's name, the firm represented, and the onsite personnel authorizing physical access on the log. Retain this log for a minimum of three months, unless otherwise restricted by law.	PE-7 VISITOR CONTROL PE-8 ACCESS RECORDS	PE
9.5 Store media back-ups in a secure location, preferably an off-site facility, such as an alternate or backup site, or a commercial storage facility. Review the location's security at least annually.	CP-6 ALTERNATE STORAGE SITE MP-4 MEDIA STORAGE	CP, MP
9.6 Physically secure all media.	CP-6 ALTERNATE STORAGE SITE MP-2 MEDIA ACCESS MP-4 MEDIA STORAGE	CP, MP
9.7 Maintain strict control over the internal or external distribution of any kind of media, including the following:	MP-2 MEDIA ACCESS MP-5 MEDIA TRANSPORT	MP
9.7.1 Classify media so the sensitivity of the data can be determined.	MP-3 MEDIA MARKING RA-2 SECURITY CATEGORIZATION	MP, RA

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
9.7.2 Send the media by secured courier or other delivery method that can be accurately tracked	MP-5 MEDIA TRANSPORT	MP
9.8 Ensure management approves any and all media that is moved from a secured area (especially when media is distributed to individuals).	N/A	
9.9 Maintain strict control over the storage and accessibility of media.	CP-6 ALTERNATE STORAGE SITE MP-2 MEDIA ACCESS MP-4 MEDIA STORAGE	CP, MP
9.9.1 Properly maintain inventory logs of all media and conduct media inventories at least annually.	N/A	
9.10 Destroy media when it is no longer needed for business or legal reasons as follows:	MP-6 MEDIA SANITIZATION MP-6-COV MEDIA SANITIZATION (COV)	MP
9.10.1 Shred, incinerate, or pulp hardcopy materials so that cardholder data cannot be reconstructed.	MP-6 MEDIA SANITIZATION MP-6-COV MEDIA SANITIZATION (COV)	MP
9.10.2 Render cardholder data on electronic media unrecoverable so that cardholder data cannot be reconstructed.	MP-6 MEDIA SANITIZATION MP-6-COV MEDIA SANITIZATION (COV)	MP
Requirement 10: Track and monitor all access to network resources and cardholder data		
10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.2 Implement automated audit trails for all system components to reconstruct the following events:	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.2.1 All individual accesses to cardholder data.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.2.2 All actions taken by any individual with root or administrative privileges.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.2.3 Access to all audit trails.	N/A	
10.2.4 Invalid logical access attempts.	AU-3 CONTENT OF AUDIT RECORDS	AU
10.2.5 Use of identification and authentication mechanisms.	N/A	
10.2.6 Initialization of the audit logs.	N/A	
10.2.7 Creation and deletion of system-level objects.	N/A	
10.3 Record at least the following audit trail entries for all system components for each event:	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.3.1 User identification.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.3.2 Type of event.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.3.3 Date and time.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
10.3.4 Success or failure indication.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.3.5 Origination of event.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	AU
10.3.6 Identity or name of affected data, system component, or resource.	AU-2 AUDITABLE EVENTS AU-3 CONTENT OF AUDIT RECORDS	
10.4 Using time synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.	AU-8 TIME STAMPS	AU
10.4.1 Critical systems have the correct and consistent time.	AU-8 TIME STAMPS	AU
10.4.2 Time data is protected.	AU-9 PROTECTION OF AUDIT INFORMATION	AU
10.4.3 Time settings are received from industry-accepted time sources.	AU-8 TIME STAMPS	AU
10.5 Secure audit trails so they cannot be altered.	AU-9 PROTECTION OF AUDIT INFORMATION	AU
10.5.1 Limit viewing of audit trails to those with a job-related need.	AU-9 PROTECTION OF AUDIT INFORMATION	AU
10.5.2 Protect audit trail files from unauthorized modifications.	AU-9 PROTECTION OF AUDIT INFORMATION	AU
10.5.3 Promptly back up audit trail files to a centralized log server or media that is difficult to alter.	AU-9 PROTECTION OF AUDIT INFORMATION	AU
10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN	AU-3 CONTENT OF AUDIT RECORDS	AU
10.5.5 Use file integrity monitoring or change detection software on logs to ensure that existing log data cannot be changed without generating alerts (although new data being added should not cause an alert).	SI-7 SOFTWARE AND INFORMATION INTEGRITY	SI
10.6 Review logs for all system components at least daily. Log reviews must include those servers that perform security functions like intrusion detection system (IDS) and authentication, authorization, and accounting protocol (AAA) servers (for example, RADIUS).	AU-6 AUDIT REVIEW, ANALYSIS, AND REPORTING	AU
10.7 Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from backup).	AU-11 AUDIT RECORD RETENTION (Library of Virginia regulates)	AU
Requirement 11: Regularly test security systems and processes		
11.1 Test for the presence of wireless access points and detect unauthorized wireless access points on a quarterly basis. Note: Methods that may be used in the process include, but are not limited to, wireless network scans, physical/logical inspections of system components and infrastructure, network access control NAC), or wireless IDS/IPS. Whichever methods are used, they must be sufficient to detect and identify any unauthorized devices.	AC-18 WIRELESS ACCESS	AC
11.2 Run internal and external network vulnerability scans at least quarterly and after any significant change in the networ (such as new system component installations, changes in network topology, firewall rule modifications, product upgrades).	RA-5 VULNERABILITY SCANNING RA-5-COV VULNERABILITY SCANNING (COV)	RA
11.2.1 Perform quarterly internal vulnerability scans.	RA-5 VULNERABILITY SCANNING RA-5-COV VULNERABILITY SCANNING (COV)	RA

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
11.2.2 Perform quarterly external vulnerability scans via an Approved Scanning Vendor (ASV) approved by the Payment Card Industry Security Standards Council (PCI SSC).	RA-5 and RA-5-COV VULNERABILITY SCANNING require vulnerability scans every 90 days but do not require ASVs perform them	RA
11.2.3 Perform internal and external scans after any significant change.	SA-3-COV-2 LIFE CYCLE SUPPORT (COV) requires post-change scans for Internet-facing sensitive system: "3.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."	SA
11.3 Perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (such as an operating system upgrade, a sub-network added to the environment, or a web server added to the environment). These penetration tests must include the following:	CA-2 SECURITY ASSESSMENTS RA-5 VULNERABILITY SCANNING	CA, RA
11.3.1 Network-layer penetration tests.	N/A	
11.3.2 Application-layer penetration tests.	N/A	
11.4 Use intrusion detection systems, and/or intrusion prevention systems to monitor all traffic at the perimeter of the cardholder data environment as well as at critical points inside of the cardholder data environment, and alert personnel to suspected compromises. Keep all intrusion detection and prevention engines, baselines, and signatures up-to-date.	IR-1-COV INCIDENT RESPONSE SI-4 INFORMATION SYSTEM MONITORING	IR, SI
11.5 Deploy file integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files or content files; and configure the software to perform critical file comparisons at least weekly.	SI-7 SOFTWARE AND INFORMATION INTEGRITY	SI
Requirement 12: Maintain a policy that addresses information security for all personnel		
12.1 Establish, publish, maintain, and disseminate a security policy that accomplishes the following:	No requirement specified	
12.1.1 Addresses all PCI DSS requirements	ALL POLICIES & CONTROLS in combination	ALL
12.1.2 Includes an annual process that identifies threats, and vulnerabilities, and results in a formal risk assessment.	RA-3 RISK ASSESSMENT	RA
12.1.3 Includes a review at least annually and updates when the environment changes.	RA-3 RISK ASSESSMENT	RA
12.2 Develop daily operational security procedures that are consistent with requirements in this specification (for example, user account maintenance procedures, and log review procedures).	NUMEROUS CONTROLS	APPENDIX - Required Process Procedures
12.3 Develop usage policies for critical technologies (for example, remote access technologies, wireless technologies, removable electronic media, laptops, tablets, personal data/digital assistants (PDAs), email usage and internet usage) and define proper use of these technologies. Ensure these usage policies require the following:	NUMEROUS CONTROLS	
12.3.1 Explicit approval by authorized parties.	3.1.1 AGENCY HEAD 3.1.3 INFORMATION SECURITY OFFICER (ISO)	SECTION 3.1 - 3.1.1, 3.1.3

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
12.3.2 Authentication for use of the technology.	ALL POLICIES & CONTROLS except AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION	ALL EXCEPT AC-14
12.3.3 A list of all such devices and personnel with access.	CM-2-COV BASELINE CONFIGURATION (COV) & CM-8 INFORMATION SYSTEM COMPONENT INVENTORY require inventory of devices but there is no requirement for identifying personnel with access	CM
12.3.4 Labeling of devices to determine owner, contact information, and purpose.	VITA SEC501-07 has no requirement for asset tags, but they are used in practice to identify device owner, contact information and location.	
12.3.5 Acceptable uses of the technology.	PL-4 RULES OF BEHAVIOR PL-4-COV RULES OF BEHAVIOR (COV)	PL
12.3.6 Acceptable network locations for the technologies.	PE-4 ACCESS CONTROL FOR TRANSMISSION MEDIUM PE-18 LOCATION OF INFORMATION SYSTEM COMPONENTS	PE
12.3.7 List of company-approved products.	N/A	
12.3.8 Automatic disconnect of sessions for remote access technologies after a specific period of inactivity.	SC-10 NETWORK DISCONNECT	SC
12.3.9 Activation of remote access technologies for vendors and business partners only when needed by vendors and business partners, with immediate deactivation after use.	N/A	
12.3.10 For personnel accessing cardholder data via remote access technologies, prohibit copy, move, and storage of cardholder data onto local hard drives and removable electronic media, unless explicitly authorized for a defined business need.	N/A	
12.4 Ensure that the security policy and procedures clearly define information security responsibilities for all personnel.	ALL POLICIES & CONTROLS in combination	ALL
12.5 Assign to an individual or team the following information security management responsibilities:	3.1.1 AGENCY HEAD 3.1.3 INFORMATION SECURITY OFFICER (ISO)	SECTION 3.1 - 3.1.1, 3.1.3
12.5.1 Establish, document, and distribute security policies and procedures.	3.1.3 INFORMATION SECURITY OFFICER (ISO)	SECTION 3.1 - 3.1.3
12.5.2 Monitor and analyze security alerts and information, and distribute to appropriate personnel.	IR-1-COV INCIDENT RESPONSE (COV) IR-4 INCIDENT HANDLING IR-5 INCIDENT MONITORING IR-5-COV INCIDENT MONITORING (COV) SI-4 INFORMATION SYSTEM MONITORING SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	IR, SI
12.5.3 Establish, document, and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.	3.1.3 INFORMATION SECURITY OFFICER (ISO)	SECTION 3.1 - 3.1.3
12.5.4 Administer user accounts, including additions, deletions, and modifications.	AC-2 ACCOUNT MANAGEMENT AC-2-COV ACCOUNT MANAGEMENT (COV)	AC

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
12.5.5 Monitor and control all access to data.	Monitor: SI-4 INFORMATION SYSTEM MONITORING Control: AC-3 ACCESS ENFORCEMENT AC-6 LEAST PRIVILEGE	AC, SI
12.6 Implement a formal security awareness program to make all personnel aware of the importance of cardholder data security.	3.1.1 AGENCY HEAD 3.1.3 INFORMATION SECURITY OFFICER (ISO) AT-2 SECURITY AWARENESS AT-2-COV SECURITY AWARENESS (COV)	AT SECTION 3.1 - 3.1.1, 3.1.3
12.6.1 Educate personnel upon hire at least annually. Note: Methods can vary depending on the role of the personnel and their level of access to the cardholder data.	3.1.1 AGENCY HEAD 3.1.3 INFORMATION SECURITY OFFICER (ISO) AT-2 SECURITY AWARENESS AT-2-COV SECURITY AWARENESS (COV)	AT, SECTION 3.1 - 3.1.1, 3.1.3
12.6.2 Require personnel to acknowledge at least annually that they have read and understood the security policy and procedures.	AT-2-COV SECURITY AWARENESS (COV) PL-4 RULES OF BEHAVIOR PS-6 ACCESS AGREEMENTS	AT, PL, PS
12.7 Screen potential personnel prior to hire to minimize the risk of attacks from internal sources. (Examples of background checks include previous employment history, criminal record, credit history and reference checks.) Note: For those potential personnel to be hired for certain positions such as store cashiers who only have access to one card number at a time when facilitating a transaction, this requirement is a recommendation only.	PS-3 PERSONNEL SCREENING	PS
12.8 If cardholder data is shared with service providers, maintain and implement policies and procedures to manage service providers, to include the following:	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS CA-3 INFORMATION SYSTEM CONNECTIONS CA-3-COV INFORMATION SYSTEM CONNECTIONS (COV) CP-6 ALTERNATE STORAGE SITE SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	AC, CA, CP, SA
12.8.1 Maintain a list of service providers.	CA-3 INFORMATION SYSTEM CONNECTIONS CA-3-COV INFORMATION SYSTEM CONNECTIONS (COV) MA-5 MAINTENANCE PERSONNEL	MA
12.8.2 Maintain a written agreement that includes an acknowledgement that the service providers are responsible for the security of cardholder data the service providers possess.	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS CA-3 INFORMATION SYSTEM CONNECTIONS CA-3-COV INFORMATION SYSTEM CONNECTIONS (COV) CP-6 ALTERNATE STORAGE SITE SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	SA
12.8.3 Ensure there is an established process for engaging service providers including proper due diligence prior to engagement.	SA-4 ACQUISITIONS	

PCI Requirements	VITA/NIST Controls	VITA / NIST Control Family
12.8.4 Maintain a program to monitor service providers' PCI DSS compliance status at least annually.	AC-20 USE OF EXTERNAL INFORMATION SYSTEMS CA-3 INFORMATION SYSTEM CONNECTIONS CA-3-COV INFORMATION SYSTEM CONNECTIONS (COV) CP-6 ALTERNATE STORAGE SITE SA-9 EXTERNAL INFORMATION SYSTEM SERVICES	SA
12.9 Implement an incident response plan. Be prepared to respond immediately to a system breach.	IR-1 INCIDENT RESPONSE IR-1-COV INCIDENT RESPONSE (COV) IR-2 INCIDENT RESPONSE TRAINING IR-3 INCIDENT RESPONSE TESTING AND EXERCISES IR-4 INCIDENT HANDLING IR-4-COV INCIDENT HANDLING (COV) IR-4-COV-2 INCIDENT HANDLING (COV-2) IR-5 INCIDENT MONITORING IR-6 INCIDENT REPORTING IR-6-COV INCIDENT REPORTING (COV) IR-7 INCIDENT RESPONSE ASSISTANCE IR-8 INCIDENT RESPONSE PLAN	IR, SI
12.9.1 Create the incident response plan to be implemented in the event of system breach. Ensure the plan addresses the following, at a minimum: § Roles, responsibilities and communication and contact strategies in the event of a compromise including notification of the payment brands, at a minimum § Specific incident response procedures § Business recovery and continuity procedures § Data back-up processes § Analysis of legal requirements for reporting compromises § Coverage and responses of all critical system components § Reference or inclusion of incident response procedures from the payment brands	CP-2 CONTINGENCY PLAN CP-9 INFORMATION SYSTEM BACKUP CP-10 INFORMATION SYSTEM RECOVERY AND RECONSTITUTION IR-6 INCIDENT REPORTING IR-6-COV INCIDENT REPORTING (COV) N/A Payment Brand specific requirements	CP, IR
12.9.2 Test the plan at least annually.	IR-3 INCIDENT RESPONSE TESTING AND EXERCISES	IR
12.9.3 Designate specific personnel to be available on a 24/7 basis to respond to alerts.	IR-1 INCIDENT RESPONSE IR-1-COV INCIDENT RESPONSE (COV)	IR
12.9.4 Provide appropriate training to staff with security breach response responsibilities.	IR-2 INCIDENT RESPONSE TRAINING	IR
12.9.5 Include alerts from intrusion detection, intrusion prevention, and file integrity monitoring systems.	IR-5 INCIDENT MONITORING IR-5-COV INCIDENT MONITORING (COV) SI-5 SECURITY ALERTS, ADVISORIES, AND DIRECTIVES	IR
12.9.6 Develop a process to modify and evolve the incident response plan according to lessons learned and to incorporate industry developments.	IR-8 INCIDENT RESPONSE PLAN	IR

DMV SECURITY ARCHITECTURE POLICY	
No.	**Requirement / Guidance**
1)	**Purpose**
	The DMV Enterprise Security Architecture Policy is designed through concepts of enhanced security and standardization to be a core set of principles required to provide maximum uptime to applications and customers interacting with the DMV infrastructure.
2)	**Scope**
	To that end, DMV's Enterprise Security Architecture Policy is a service-based architecture utilizing a variety of techniques to provide this service level. DMV provides high-availability services to the mainframe, databases, and a variety of other DMV systems through this infrastructure.
	All person or entities authorized to transact business, access, use, provide, or receive information contained in any DMV information system, record set, or electronic communication system are subject to this policy.
	This includes, but is not limited to:
a)	Employees (full-time, part-time, wage employees),
b)	Contracted personnel (contractors, consultants, vendors, or temps),
c)	Non-employees (volunteers or interns).
3)	**Background**
	DMV's Security Architecture Policy is based on the multi-tier application deployment model and a multi-level security model. These models provide a disconnect between user activity and the secured information that DMV maintains. The DMV's Security Architecture Policy provides methods to programmatically access information stored in DMV databases, host (mainframe) systems, and file stores. These methods provide risk mitigation and confidence that data is protected and accurate when accessed and delivered. It also provides a means to audit what data was accessed and by whom.
	DMV's Security Architecture Policy, from a security perspective, is based on the security principles of "Least Privilege". The security model employed is based on best practices published by the NSA, NIST, Center for Internet Security and accredited security organizations such as ISC2 and SANS. These defined security models are applied to workstations, servers, applications and other elements of the infrastructure.
	DMV is very restrictive with security policies. DMV only provides detailed security information on an as-needed basis. DMV will decide which security information is to be shared or released based on Commonwealth of Virginia security and architecture policy and DMV Information Security Policy.
	DMV follows the guidelines provided in the Commonwealth of Virginia (COVA) Information Technology ITRM Security policies, standards and guidelines. The reference URL for these ITRM directives are found at: http://www.vita.virginia.gov/library/default.aspx?id=537 under the Information Security heading.
	Additionally, Commonwealth ITRM Enterprise Architecture guidance is found at: http://www.vita.virginia.gov/oversight/default.aspx?id=365.
	Additionally, please review both of these sources of security architecture governance by reference to the templates and documentation for non-ITRM security found at http://www.vita.virginia.gov/library/default.aspx?id=5520#security .
	With the passage of time, the exact URL may be changed, however the DMV governance process will published corrections to these URLs as they may be superseded, however vendors and other parties are to refer the ITRM and non-ITRM sections of the VITA Partnership Library http://www.vita.virginia.gov/library/ for current information as it is needed.
	In addition to Commonwealth of Virginia sources of security architecture, the requirements for development and implementations of security and architecture controls have been developed by reference to NIST Special Publication 800-53, revision 1. Over time different elements of these controls may be redacted or incorporated without notice.
	All security and architecture guidelines published by the Commonwealth of Virginia and the Virginia Department of Motor Vehicles must be followed with current and proposed solutions. These requirements are set forth in the following subheadings below.
4)	**General Security Architecture Policy Requirements:**
a)	DMV does not allow direct connections from outside sources to internal systems. **VITA - SC-7 Boundary Protection** **PCI - 1.3** Prohibit direct public access between the Internet and any system component in the cardholder data environment (including requirements 1.3.1-1.3.5, 1.3.7).

No.	Requirement / Guidance
b)	DMV requires multi-level security models for risk minimization. For reference see: http://en.wikipedia.org/wiki/Multilevel_security. **VITA - N/A** **PCI - 2.2.1** Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. This requires segregation of differing risk levels using accepted techniques for security compartmentalization.
c)	All externally and most internally available applications are designed in a multi-tier security model. The tiers are hosted on separate hardware resources and are separated by independent firewalls. These are not application layers but independent operational tiers that only can communicate with one another in distinct and prescribed ways. **VITA - SA-3-COV-2 LIFE CYCLE SUPPORT (COV-2)** **PCI - N/A** For reference information on the multi-tier security model please refer to:
i)	http://en.wikipedia.org/wiki/Multitier_architecture,
d)	No http proxy based applications are allowed.
e)	DMV restricts the IP application ports that are allowed to traverse networks and segments. It should not be assumed by an application has access to any port unless this security architecture policy specifically describes such interaction.
f)	DMV does not allow dynamic port allocation applications.
g)	DMV considers any machine that is directly accessed by an outside entity as a perimeter device and restricts accordingly.
h)	DMV does not allow the sharing of security credentials for user access to DMV systems. This includes both DMV internal users and external users.
i)	DMV restricts network services that traverse LAN and WAN networking segments.
j)	Direct remote access to any computer is not allowed.
k)	Standalone modems are not allowed
l)	Vendor provided remote control applications are not allowed.
m)	Servers and User PC's are restricted from residing on the same network segment.
n)	Any proposed system or optional configuration must have an automatic restart process for connection failures or if the back end systems are unavailable.
o)	System must provide future growth estimates and hardware requirements to support future growth and scalability.
p)	Any proposed system or optional configuration that requires a CSC Local Server must utilize a Virtual Server running on VMWare ESX Server. Application must support current releases of VMWare ESX Server. No physical server will be allowed to be deployed locally to CSCs. Desktop systems are not utilized to provide server type services.
q)	Any proposed system or optional configuration must work with the product licensed by Citrix Essentials for XenServer (Provisioning) [known as Ardence Desktop Edition Streamed Operating System] product.
r)	Any customer record information that is access must be encrypted via known industry security methodologies and be fully documented.
s)	DMV does not deploy any Middleware clients (i.e. ODBC, Oracle, or SQL Server Client) to the servers unless it is a Business Logic tier server.
t)	Any proposed system or optional configuration must conform to the DMV Base Network Configuration that will be defined as VITA Partnership transforms our current network infrastructure.
5)	**Application Authentication Security Architecture Policy**
	Application authentication is handled differently based on where the application provides services and the characteristics of the service provided. Application Authentication & Authorization is provided by the following means based on specific use:
a)	DMV requires one of the authentication methods be selected by all current or proposed applications. No standalone user database are allowed without one of these authentication methods:
i)	Microsoft Active Directory: Internal Application Authentication. This is not A/D synchronization resulting in an application user store and an A/D user store, but is consumption of the application of the existing A/D groups. Microsoft Active Directory usage is a Commonwealth authentication standard.
ii)	DMV Employee PIN: Internal Application Authentication. Typically HTTP based applications.
iii)	RSA SecurID FOB access: External Applications provided via DMV's web site, extranet system applications, and remote access for DMV Employees and trusted contractors.
iv)	Future - the implementation of consumer based multi-factor based on security risk is being considered for implementation.
b)	**VITA - IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)**
	Control: The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users).

No.	Requirement / Guidance
i)	**PCI:** 8.1 Assign all users a unique username before allowing them to access system components or cardholder data. 8.2 In addition to assigning a unique ID, employ at least one of the following methods to authenticate all users: § Something you know, such as a password or passphrase § Something you have, such as a token device or smart card § Something you are, such as a biometric
c)	**VITA - IA-4 IDENTIFIER MANAGEMENT**
	Control: The organization manages information system identifiers for users and devices by: Receiving authorization from a designated organizational official to assign a user or device identifier; Selecting an identifier that uniquely identifies an individual or device; Assigning the user identifier to the intended party or the device identifier to the intended device; Preventing reuse of user or device identifiers for a period of one-year at a minimum; and Disabling the user identifier after 90-days of inactivity.
i)	**PCI:** 8.1 Assign all users a unique username before allowing them to access system components or cardholder data. 8.5 Ensure proper user identification and authentication management for non-consumer users and administrators on all system components as follows: 8.5.1 Control addition, deletion, and modification of user IDs, credentials, and other identifier objects. 8.5.5 Remove/disable inactive user accounts at least every 90 days.
d)	**VITA - IA-6 AUTHENTICATOR FEEDBACK**
	Control: The information system obscures feedback of authentication information during the authentication process to protect the information from possible exploitation/use by unauthorized individuals.
i)	**PCI:** PCI-DSS has no requirement for this control.
6)	**Remote Access Authentication Security Architecture Policy**
a)	Remote access to the current or proposed system will be provided by devices and means identified by the IT Security Director (Information Security Officer - ISO). Currently VPN connections are provided using a DMV provided SecureID security key FOB.
b)	SecureID key FOBs are issued to individuals and may not be shared with anyone other then those specifically designated. There may be other acceptable use criteria associated with these key FOBs.
c)	For vendor requested connections to DMV, DMV will provide the remote access software that will be used. This software will allow the Vendor to remotely administer the servers related to their product.
d)	Currently DMV uses RSA SecurID for access and authentication and Virtual Network Computing or Microsoft Terminal Services for remote access software.
e)	Remote Data transfer connections must be secured via VPN or a method approved of by a security classification and sensitivity assessment by the DMV IT Security Director (Information Security Officer - ISO). These connections are regarded as severely restricted which will be treated as perimeter connections and firewalled with security applied accordingly.
f)	**VITA - AC-17 REMOTE ACCESS & AC-17-COV REMOTE ACCESS (COV)**
i)	**PCI -** 2.3 Encrypt all non-console administrative access using strong cryptography. Use technologies such as SSH, VPN, or SSL/TLS for web-based management and other non-console administrative access. 4.1 Use strong cryptography and security protocols (for example, SSL/TLS, IPSEC, SSH, etc.) to safeguard sensitive cardholder data during transmission over open, public networks. 8.3 Incorporate two-factor authentication for remote access (network-level access originating from outside the network) to the network by employees, administrators, and third parties. (For example, remote authentication and dial-in service (RADIUS) with tokens; terminal access controller access control system (TACACS) with tokens; or other technologies that facilitate two-factor authentication.) 8.5.6 Enable accounts used by vendors for remote access only during the time period needed. Monitor vendor remote access accounts when in use.
7)	**Platform Infrastructure Security Architecture Policy**
	Platform Infrastructure Description
	Previously the Security Architecture Policy, described how a multi-tiered security model is used. This security Policy also includes multi-level security aspects that protect data on one level from data on another level.

No.	Requirement / Guidance
	DMV utilizes Windows based servers as Presentation, Business Logic, and Data Access servers. DMV Servers are secured based on current industry standards provided by the NSA, SANS Institute, etc, as well as those published by VITA. Servers are designed with standardization across all machines. DMV utilizes both physical and virtual servers (VMWare ESX Server) based on need and activity.
	DMV employs the use of Mainframe Legacy systems for transactions relating to COVA citizen records and various Motor Carrier services. Currently, user access to these systems is delivered by TN3270 and HTTP/HTTPS based applications.
	Document and Image management, storage, retrieval, and workflow services are provided by the Hyland Systems Onbase application. DMV utilizes Microsoft Exchange and Outlook for email and personal productivity functions including calendars, meeting scheduling, etc.
	The following are requirements for the platform infrastructure (multi-tiered and multi-level security) implemented at DMV for all systems:
a)	General tier requirement: NO direct access to any Data Access Tier information or services is allowed from either the Client or Presentation tiers.
b)	General tier requirement: All tiers are separated by firewall access control list rules
c)	General tier requirement: The presentation of an application to a client (whether as a separate application, as a browser-based presentation, or as another type of client device) is not to be counted as a presentation tier. The concept of a presentation tier is a hosted instance and is not a browser/client presentation of a user interface. The presentation tier is some instances would be the web server hosting the user interface to a web browser. It would not be the web browser itself. Additionally, terminal services as a client is not a tier, but a terminal services server hosting terminal services to connected clients would be a tier.
d)	General tier requirement: Applications must be architected in an n-tier configuration with at least 3 tiers (presentation, business logic, and data access).
i)	A tier is not solely a software layer.
ii)	A tier (see references above in 6) Background) is required to run on separate hardware resources and connections between such tiers are proxied through firewall and other security access.
iii)	It is not allowed to have 2 software layers compiled and running on one tier (i.e. Presentation and Business logic layers running on Business Logic tier, or Business Logic and Data Layers running on Business Logic tier etc.).
iv)	A tier is determined by operational separation (hosting) not by how a software layers is used (i.e. Hosting of the product or application requires a minimum of 3 tiers; it is not an optional component).
e)	Direct connections through tiers (i.e. client directly to data) are not permitted.
i)	Access to the different tiers must be capable of being fully proxied. No tunneling or proprietary transport mechanisms are to be utilized.
ii)	Each tier MUST have a documented and full featured API utilizing industry standard interfaces that are fully compatible with DMV's application infrastructure. This API must be licensed and available for DMV consumption.
iii)	Communications between tiers should be TCP/IP port based connections.
iv)	Application integration must occur via an API based Programmatic Methodology. "Screen Scraping" and HLLAPI techniques are not permitted.
f)	General tier requirement: Data transfer connections are subject to data access limitations described in the Application Tier structure presented in the Security Architecture Policy System Description and must be designed according to these requirements.
g)	DMV Architecture Security Policy tier structure:
i)	Client Tier: Application front-end run by the user. Typically a web browser or smart client. This layer does not count as a tier/separation in determining if a tier is 3-tier or n-tier compatible.
ii)	Presentation Tier: Content displayed to the user. IIS web server. This includes all UI access presented for client input and evaluation. Presentation tier to Business Logic Tier is physical hardware resource separation through a firewall. It is not permitted that a presentation application layer exists on a services or data tier.
iii)	Business Logic Tier: Middleware layer that provides connectivity to backend systems for the Presentation Tier. This includes all business logic that is evaluated for decisions to process data. Business Logic Tier to Data Tier is physical hardware resource separation through a firewall. It is not permitted that business logic be presented on the presentation tier. It is not permitted that business logic exist as data in the data tier. It is not permitted that data be stored on the Business Logic tier.
iv)	Data Access Tier: Layer that provides data storage for DMV information. Databases, Host Systems, Files Storage, etc. This includes all data that is owned by the data owner of record for a DMV sensitive or non-sensitive system. Business Logic Tier to Data Tier is physical hardware resource separation through a firewall. It is not permitted that data be stored or maintained on a business logic or the presentation tier. It is not permitted that business logic exist as data in the data tier. It is not permitted that data be stored on the Business Logic tier.
8)	**Application Development Security Architecture Policy**
a)	DMV does not deploy any Java revisions on the Enterprise Application Infrastructure servers.

No.	Requirement / Guidance
b)	DMV does not deploy any Middleware clients (i.e. ODBC, Oracle, or SQL Server Client) to the servers unless it is a Business Logic tier server.
c)	DMV provides custom components to access the Data Access stores in place of the standard DACs provided by Microsoft.
d)	DMV prefers data access to be performed via web services through the Business Logic tier, but offers other custom components as an alternative for high-volume data access through the Business Logic tier.
e)	Application access to these COV legacy systems for access to COV customer records of account is provided by an API based programmatic approach or web services that are supplied by the Business Logic tier. Customer records of account are controlled by business decisions made by the system and data owners of record.
f)	Applications must not utilize any proprietary storage format and/or encryption routines that are not readily available for use by DMV's development staff to integrate applications with existing and/or new systems.
g)	Screen scraping or macro based solutions are not allowed. All communication to other systems must take place via a programmatic approach.
h)	Any proposed system or optional configuration and associated peripherals must be compliant with and utilize the Onbase system for, at a minimum, document acquisition, storage, workflow, and retrieval. DMV is licensed to utilize the Onbase application API for building custom interfaces to Onbase.
i)	**VITA - SA-3 LIFE CYCLE SUPPORT**
	Control: The organization: a. Manages the information system using a system development life cycle methodology that includes information security considerations; b. Defines and documents information system security roles and responsibilities throughout the system development life cycle; and c. Identifies individuals having information system security roles and responsibilities.
i)	**PCI:** 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.4.2 Separation of duties between development/test and production environments. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes; as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements.
j)	**VITA - SA-3-COV-2 LIFE CYCLE SUPPORT (COV-2)**
	Control: Each agency ISO is accountable for ensuring the following steps are documented and followed: Application Planning Application Development Production and Maintenance Please refer to control for full details on each area.
i)	**PCI:** 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle. 6.3.2 Review of custom code prior to release to production or customers in order to identify any potential coding vulnerability. 6.4 Follow change control processes and procedures for all changes to system components. The processes must include the following: 6.4.1 Separate development/test and production environments. 6.4.3 Production data (live PANs) are not used for testing or development. 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes; as industry best practices for vulnerability management are updated (for example, the OWASP Guide, SANS CWE Top 25, CERT Secure Coding, etc.), the current best practices must be used for these requirements. 6.5.4 Insecure communications. 7.2 Establish an access control system for systems components with multiple users that restricts access based on a user's need to know, and is set to "deny all" unless specifically allowed. 7.2.3 Default "deny-all" setting. For sensitive, internet-facing applications only: 11.2.3 Perform internal and external scans after any significant change
k)	**VITA - SC-2 APPLICATION PARTITIONING**

No.	Requirement / Guidance
	Control: The information system separates user functionality (including user interface services) from information system management functionality.
i)	**PCI:** 8.5.16 Authenticate all access to any database containing cardholder data. This includes access by applications, administrators, and all other users. Restrict user direct access or queries to databases to database administrators.
l)	**VITA - SC-3 SECURITY FUNCTION ISOLATION**
	Control: The information system isolates security functions from nonsecurity functions.
i)	PCI: PCI-DSS has no requirement for this control.
m)	**VITA - SC-4 INFORMATION IN SHARED RESOURCES**
	Control: The information system prevents unauthorized and unintended information transfer via shared system resources.
i)	PCI: PCI-DSS has no requirement for this control.
9)	**Personnel Roles required by the above Security Architecture requirements**
	DMV separates many administrative roles to ensure that proper staff requirements and expertise are utilized effectively.
	Application Administrator/Supervisor
	The designated user to administer the application side of the solution. This user would not have direct console access to the system servers. This user would typically be an area supervisor or manager.
	Server Administrator
	Typically responsible for the Hardware and Operating systems on Network Services Servers.
	Would be responsible for:
i)	Server hardware and operating system configuration and maintenance
ii)	Server system disaster recovery
iii)	Network account management
iv)	Network access
v)	Server health monitoring
	Database Administrator
	Would be responsible for:
i)	Database table configuration
ii)	Database table access
iii)	Database administration
iv)	Database disaster recovery
	Software Development
	Would be responsible for application design and maintenance. Would not be expected to manage applications.
10)	**VITA / PCI Specific requirements**
a)	**VITA - AU-2 AUDITABLE EVENTS**
	Control: The organization: Determines, based on a risk assessment and mission/business needs, that the information system must be capable of auditing the following events: authenticated individual, access time, source of access, duration of access, and actions executed.
i)	**PCI:** 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data. 10.2.2 All actions taken by any individual with root or administrative privileges. 10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification. 10.3.2 Type of event. 10.3.3 Date and time. 10.3.4 Success or failure indication. 10.3.5 Origination of event. 10.3.6 Identity or name of affected data, system component, or resource.

No.	Requirement / Guidance
b)	**VITA - AU-3 CONTENT OF AUDIT RECORDS**
	Control: The information system produces audit records that contain sufficient information to, at a minimum, establish what type of event occurred, when (date and time) the event occurred, where the event occurred, the source of the event, the outcome (success or failure) of the event, and the identity of any user/subject associated with the event.
i)	**PCI:** 10.1 Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user. 10.2 Implement automated audit trails for all system components to reconstruct the following events: 10.2.1 All individual accesses to cardholder data. 10.2.2 All actions taken by any individual with root or administrative privileges. 10.3 Record at least the following audit trail entries for all system components for each event: 10.3.1 User identification. 10.3.2 Type of event. 10.3.3 Date and time. 10.3.4 Success or failure indication. 10.3.5 Origination of event. 10.3.6 Identity or name of affected data, system component, or resource. 10.5.4 Write logs for external-facing technologies onto a log server on the internal LAN.
c)	**VITA - CM-7 LEAST FUNCTIONALITY**
	Control: The organization configures the information system to provide only essential capabilities and specifically prohibits or restricts the use of the following functions, ports, protocols, and/or services that are not required for the business function of the information system.
	DMV-Specific Requirements: DMV configures the information system based on the security principles of “Least Privilege”. The security model employed is based on best practices published by the NSA, NIST, Center for Internet Security and accredited security organizations such as ISC2 and SANS. These defined security models are applied to workstation, servers, applications and other elements of the infrastructure. 1. DMV does not allow direct connections from outside sources to internal systems. 2. DMV requires multi-level security models for risk minimization. 3. All externally and most internally available applications are designed in a multi-tier security model. The tiers are hosted on separate hardware resources and are separated by independent firewalls. These are not application layers but independent operational tiers that only can communicate with one another in distinct and prescribed ways. 4. No http proxy based applications are allowed. 5. DMV restricts the IP application ports that are allowed to traverse networks and segments. It should not be assumed by an application has access to any port unless this security architecture policy specifically describes such interaction. 6. DMV does not allow dynamic port allocation applications. 7. DMV considers any machine that is directly accessed by an outside entity as a perimeter device and restricts accordingly. 8. DMV does not allow the sharing of security credentials for user access to DMV systems. This includes both DMV internal users and external users. 9. DMV restricts network services that traverse LAN and WAN networking segments. 10. Direct remote access to any computer is not allowed. 11. Standalone modems are not allowed 12. Vendor provided remote control applications are not allowed. 13. Servers and User PC’s are restricted from residing on the same network segment. 14. Any proposed system or optional configuration must have an automatic restart process for connection failures or if the back end systems are unavailable. 15. System must provide future growth estimates and hardware requirements to support future growth and scalability. 16. Any customer record information that is accessed must be encrypted via known industry security methodologies and be fully documented.

No.	Requirement / Guidance
i)	**PCI:** 1.1.5 Documentation and business justification for use of all services, protocols, and ports allowed, including documentation of security features implemented for those protocols considered to be insecure. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. 2.2 Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. 2.2.1 Implement only one primary function per server to prevent functions that require different security levels from co-existing on the same server. (For example, web servers, database servers, and DNS should be implemented on separate servers.) 2.2.2 Enable only necessary and secure services, protocols, daemons, etc. as required for the function of the system. 2.2.4 Remove all unnecessary functionality, such as scripts, drivers, features, subsystems, file systems, and unnecessary web servers.
d)	**VITA - IA-7 CRYPTOGRAPHIC MODULE AUTHENTICATION**
	Control: The information system uses mechanisms for authentication to a cryptographic module that meet the requirements of applicable laws, directives, policies, regulations, standards, and guidance for such authentication.
i)	**PCI:** 6.5.3 Insecure cryptographic storage.
e)	**VITA - SA-8 SECURITY ENGINEERING PRINCIPLES**
	Control: The organization applies information system security engineering principles in the specification, design, development, implementation, and modification of the information system.
i)	**PCI:** 6.3 Develop software applications (internal and external, and including web-based administrative access to applications) in accordance with PCI DSS (for example, secure authentication and logging) and based on industry best practices. Incorporate information security throughout the software development life cycle.
f)	**VITA - SC-7 BOUNDARY PROTECTION**
	Control: The information system: Monitors and controls communications at the external boundary of the system and at key internal boundaries within the system; and Connects to external networks or information systems only through managed interfaces consisting of boundary protection devices arranged in accordance with an organizational security architecture.
i)	**PCI:** 1.1.3 Requirements for a firewall at each Internet connection and between any demilitarized zone (DMZ) and the internal network zone. 1.2 Build firewall and router configurations that restrict connections between untrusted networks and any system components in the cardholder data environment. 1.2.1 Restrict inbound and outbound traffic to that which is necessary for the cardholder data environment. 1.3 Prohibit direct public access between the Internet and any system component in the cardholder data environment. 1.3.1 Implement a DMZ to limit inbound traffic to only system components that provide authorized publicly accessible services, protocols, and ports. 1.3.2 Limit inbound Internet traffic to IP addresses within the DMZ. 1.3.3 Do not allow any direct connections inbound or outbound for traffic between the Internet and the cardholder data environment. 1.3.4 Do not allow internal addresses to pass from the Internet into the DMZ. 1.3.5 Do not allow unauthorized outbound traffic from the cardholder data environment to the Internet. 1.3.7 Place system components that store cardholder data (such as a database) in an internal network zone, segregated from the DMZ and other untrusted networks. 1.4 Install personal firewall software on any mobile and/or employee-owned computers with direct connectivity to the Internet (for example, laptops used by employees), which are used to access the organization's network. 6.6 For public-facing web applications, address new threats and vulnerabilities on an ongoing basis and ensure these applications are protected against known attacks by either of the following methods: § Reviewing public-facing web applications via manual or automated application vulnerability security assessment tools or methods, at least annually and after any changes § Installing a web-application firewall in front of public-facing web applications
g)	**VITA - SI-10 INFORMATION INPUT VALIDATION**

No.	Requirement / Guidance
	Control: The information system checks the validity of information inputs.
i)	**PCI:** 6.5 Develop applications based on secure coding guidelines. Prevent common coding vulnerabilities in software development processes, to include the following: 6.5.1 Injection flaws, particularly SQL injection. Also consider OS Command Injection, LDAP and XpPath injection flaws as well as other injection flaws. 6.5.2 Buffer overflow.
h)	**VITA - SC-28 PROTECTION OF INFORMATION AT REST**
	Control: The information system protects the confidentiality and integrity of information at rest.
i)	**PCI:** 1.2.2 Secure and synchronize router configuration files. 1.3.8 Do not disclose private IP addresses and routing information to unauthorized parties. 3.4 Render PAN unreadable anywhere it is stored (including on portable digital media, backup media, and in logs) by using any of the following approaches: § One-way hashes based on strong cryptography (hash must be of the entire PAN) § Truncation (hashing cannot be used to replace the truncated segment of PAN) § Index tokens and pads (pads must be securely stored) § Strong cryptography with associated key management processes and procedures 3.4.1 If disk encryption is used (rather than file- or column-level database encryption), logical access must be managed independently of native operating system access control mechanisms (for example, by not using local user account databases). Decryption keys must not be tied to user accounts. 8.4 Render all passwords unreadable during transmission and storage on all system components using strong cryptography.

Information Security Terms and Concepts

Application System

A program (or set of programs) that performs a function directly for a user. Users generally interact with applications through a set of screens or commands. An application can be designed for specific user tasks, such as word processing, database management, or e-mail; and applications can be built to perform many business-related tasks, such as CSS, Fuels Tax, Accounts Payables, etc. Applications are different from system software, which run and control the computer system, such as the operating system - i.e., Windows XP, UNIX, etc.

Computer Network

Two or more computers that can share information typically connected by cables, data lines, or satellite links, or wireless connections.

Custodians

Organizations or individuals with delegated responsibility for protecting information by its owner. For DMV's data and information, these duties are performed by ITS, the Virginia Information Technologies Agency, and authorized third parties.

Electronic Communication Systems

System used as a means to send and receive messages electronically through connected computer systems or the Internet, such as e-mail, voice mail, wireless devices (e.g., PDAs), etc.

Employee PIN

The employee PIN (Personal Identification Number) is a four-digit code that provides users with confidential access to secure areas of MyDMV (the Intranet) when used with a DMV logon ID and their birth date. You must go to the Secure Applications page to request or use your employee PIN.

Upon requesting or changing your employee PIN, it will be sent to you by return e-mail. You will need to personalize your employee PIN within 30 days or it will expire. Be sure to keep your employee PIN in a safe place and do not share it with others. If you ever experience any difficulties or error messages when using your employee PIN, contact **SSG Help Desk** @ 804-497-7124 for assistance.

Information Security Terms and Concepts

Executives and Management Personnel

Executives, administrators, directors, division managers, and district managers are considered supervisory personnel, but they are also responsible for consistent enforcement of DMV security policies and procedures throughout their administration or assigned areas of accountability.

Extranet

A private network that is connected to organizations via the Internet but is not accessible to the general public, which allow vendors and business partners to access an organization's web site. Access to an extranet can only be obtained with a valid username and password.

Information

All data, active and inactive records and documents, regardless of form, contained in or processed by the agency and its facilities.

Intranet (MyDMV)

A private network inside a company or organization that uses the same kinds of software as found on the public Internet, but that is only for internal use. DMV's Intranet is accessible by all users in DMV, but there are various secured applications that require an Employee PIN for access. Access to secured applications must be requested by a user's supervisor via the System Access Request (SAR 13) form.

Internet (The WEB)

This is an international network of independent computer systems. The World Wide Web is one of the most recognized means of using the Internet, and the specific points where information is stored and viewed are called Web sites or Web pages. Much of the Internet is freely accessible by anyone with a PC, a modem, and a connection to an ISP (Internet Service Provider - i.e., AOL, MSN, Earthlink Comcast, etc.). However, not all sites are suitable for access for business purposes, which is the primary use of the Internet at DMV.

Information Security Terms and Concepts

LAN (Local Area Network)

A network that connects computers in a relatively small, predetermined area (such as a room, a building, or a set of buildings). Workstations and personal computers in an office are commonly connected in a LAN. This allows individual users to send or receive files and to share access to files and data.

Owners of Records and Systems

Persons who provide direction on how an organization's records and systems should be used and who should be able to gain access to them. Direction for the use of records and systems that owners provide may come from other organizations through laws, regulations, policies, or standards. At DMV, the Commissioner is the owner of all information and data originating in and stored in DMV and its information systems. In addition, the Commissioner also delegates ownership responsibilities to others based on business needs.

Record

The following are characteristics of records created, processed, or stored by DMV:

- information or a description of an event which is written on paper, stored on a computer, or recorded on audio or video tape,
- information about someone which is stored by the police, a doctor, or other official, and
- facts that are known about a person or a company and the actions they have done in the past.

Supervisory Personnel

In addition to being users themselves, supervisory personnel are responsible for overseeing the work of others and for managing the system accesses of those whom they oversee.

System Access Levels

Access levels consist of a collection of screen names or system functions. They are established in most of DMV's application systems to provide a separation of duties between work units and individual users within work units or CSCs.

System Access Request Form (SAR 13)

This is the form that DMV supervisory personnel use to request access (new, modify, terminate, transfer, suspend) to systems for users in their work areas.

Information Security Terms and Concepts

Users

All persons or entities authorized to transact business, access, use, provide, or receive information contained in any DMV information system, record set, or electronic communication system are subject to DMV's information security policy. The following are the categories of user relationships covered by this policy:

- employees (full-time and part-time (wage) employees),
- contracted personnel (contractors, consultants, vendors, or temps),
- non-employees (volunteers or interns),
- personnel who supervise others
- executive and management personnel,
- custodians,
- contracted providers of DMV services (On-line dealers, Fleet management, etc.)
- information use agreement holders, and
- memoranda of understanding holders.

Information Security Glossary

The COV IT Glossary is located on the ITRM Policies, Standards and Guidelines web page at http://www.vita.virginia.gov/library/default.aspx?id=537 .

Information Security Acronyms

AITR: Agency Information Technology Resource

BIA: Business Impact Analysis

CAP: Corrective Action Plan

CIO: Chief Information Officer

CISO: Chief Information Security Officer

COOP: Continuity of Operations Plan

DHRM: Department of Human Resource Management

DRP: Disaster Recovery Plan

FTP: File Transfer Protocol

HIPAA: Health Insurance Portability and Accountability Act

IDS: Intrusion Detection Systems

IPS: Intrusion Prevention Systems

ISO: Information Security Officer

ISO/IEC: International Organization for Standardization/

International Electrotechnical Commission

ITIES: Information Technology Investment and Enterprise

ITRM: Information Technology Resource Management

MOU: Memorandum of Understanding

PCI: Payment Card Industry

PDA: Personal Digital Assistant

PI: Personal Information

PIN: Personal Identification Number

RA: Risk Assessment

Information Security Acronyms

RPO: Recovery Point Objective

RTO: Recovery Time Objective

SDLC: Systems Development Life Cycle

Solutions Directorate (VITA)

SSID: Service Set Identifier

SSP: Security Program Plan

VDEM: Virginia Department of Emergency Management

VITA: Virginia Information Technologies Agency

IT System and Data Sensitivity Classification Template

Please see the current version of VITA ITRM SEC506 *Risk Assessment Guideline*, section 4 detailed instructions on use of this form.

General Instructions

1) Identify the types of data processed by each agency-owned IT system. The designation of these data types may be unique to each agency and should be specific enough to provide clear differentiation among various types of data. Types of data, for example, may include personnel records, customer information, and public information, among others.

2) Determine if the data is subject to regulation by other agencies (Commonwealth or Federal), customer agency requirements, or other external requirements.

3) For each type of data, determine the level of impact of a compromise of :

- **confidentiality**, which addresses the impact of unauthorized disclosure;
- **integrity**, which addresses the impact of unauthorized modification; and
- **availability**, which addresses the impact of outages, and is defined by the BIA.

Once the level of impact of a compromise is determined, classify the impact on the agency's mission, for each of the criteria of confidentiality, integrity and availability. Sensitivity classifications may be unique to each agency and should be specific enough to enable the agency to determine appropriate levels of protection for IT systems and data.

One method is to rate the impact of a compromise to confidentiality, integrity, and availability as "high", "moderate" or "low".

- **High** – *If compromised, the agency cannot perform a major portion of its mission*.
- **Moderate** – *If compromised, all elements of the agency mission can continue, but with significant degradation in quality or timeliness of information and service.*
- **Low**– *If compromised, all elements of the agency mission can continue with no visible adverse effect to agency customers*.

	Sensitivity		
Type of Data	***Confidentiality***	***Integrity***	***Availability***

IT System Inventory and Definition Template

Please see the current version of VITA ITRM SEC506 *Risk Assessment Guideline*, section 5 detailed instructions on use of this form.

IT System Inventory and Definition Document				
I. IT System Identification and Ownership				
IT System ID		**IT System Common Name**		
Owned By				
Physical Location				
Major Business Function				
System Owner **Phone Number**		**System Administrator(s)** **Phone Number**		
Data Owner(s) **Phone Number(s)**		**Data Custodian(s)** **Phone Number(s)**		
Other Relevant Information				
II. IT System Boundary and Components				
IT System Description and Components				
IT System Interfaces				
IT System Boundary				
III. IT System Interconnections (add additional lines, as needed)				
Agency or Organization	**IT System Name**	**IT System ID**	**IT System Owner**	**Interconnection Security Agreement Status**
IV. IT System and Data Sensitivity (add additional lines, as needed)				

Type of Data	Sensitivity Ratings Include Rationale for each Rating		
	Confidentiality	**Integrity**	**Availability**

Overall IT System Sensitivity Rating and Classification	**Overall IT System Sensitivity Rating** Must be "high" if sensitivity of any data type is rated "high" on any criterion
	↑ **High** ↑ **Moderate** ↑ **Low**
	IT System Classification Must be "Sensitive" if overall sensitivity is "high"; consider as "Sensitive" if overall sensitivity is "moderate"
	↑ **Sensitive** ↑ **Non-Sensitive**

Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media

The *Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media* form follows this page.

Authorization to Store Sensitive Data
on a Mobile Data Storage Device or Media

I hereby, authorize the storage of the following sensitive data on the designated mobile data storage device or media:

The business reasons driving this requirement are the needs to:

The mitigating controls in place are the requirements of the *DMV IT Security Policy* and include:

1. All mobile data storage devices/media shall be protected with strong passwords; and
2. All sensitive data shall be encrypted; and
3. All mobile data storage devices/media containing sensitive data shall be kept under the user's physical control at all times.

Additional mitigating controls include:

The requestor recognizes that the data is sensitive and accepts the risks of storage on the designated mobile data storage medium listed above.

This authorization expires one (1) year from the approval date of the Commissioner.

Requestor Information	
Printed Name:	
Signature:	
Date:	
Title:	
Department:	
Telephone Number:	

IT Security Director/ISO Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	☐ YES - Request is Approved ☐ NO - Request is Not Approved

Assistant Commissioner/CIO Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	☐ YES - Request is Approved ☐ NO - Request is Not Approved

Commissioner Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	☐ YES - Request is Approved ☐ NO - Request is Not Approved

Return Original Form to IT Security Director after Commissioner Review/Approval