

VIRGINIA DEPARTMENT OF MOTOR VEHICLES

IT SECURITY POLICY

Version 1.7
February 13, 2009



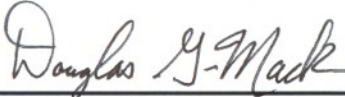
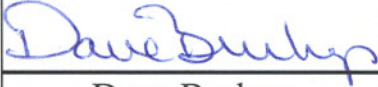

<i>Approval</i>	5
<i>Revision History</i>	6
1.0 Introduction	7
1.1 Overview	7
1.2 Review	7
1.3 Policy/Legal Conflicts	7
1.4 Exceptions	8
1.5 Enforcement	8
1.6 Policy Non-Enforcement	8
1.7 Violation of Law	8
1.8 Authority	8
1.9 Freedom of Information (FOIA)	9
2.0 Policy Implementation	10
2.1 Purpose	10
2.2 Scope	10
2.3 Policy	10
2.3.1 Goal	10
2.3.2 IT Security Policy Development and Direction	11
2.3.3 Management Security Approach	11
2.3.4 Information Security Resources	11
2.3.5 Systems Administrators Don't Handle Security Administration	11
2.3.6 Disabling Critical Security Components	11
2.3.7 Information Security Compliance	12
2.3.8 Effective Date of DMV IT Security Policy	12
2.3.8.1 Approved by Commissioner	12
2.3.8.2 Exceptions	12
3.0 Policies	12
3.1 Risk Management	12
3.1.1 Purpose	12
3.1.2 IT Security Roles and Responsibilities	13
3.1.2.1 Purpose	13
3.1.2.2 Requirements	13
3.1.2.3 DMV IT Security Roles	14
3.1.3 Business Impact Analysis	18
3.1.3.1 Purpose	18
3.1.3.2 Requirements	19
3.1.4 IT System and Data Sensitivity Classification	20
3.1.4.1 Purpose	20
3.1.4.2 Sensitive Data as Defined by DMV	20
3.1.4.3 Requirements	20
3.1.5 Sensitive IT System Inventory and Definition	22
3.1.5.1 Purpose	22
3.1.5.2 Requirements	22
3.1.6 Risk Assessment	23
3.1.6.1 Purpose	23

3.1.6.2 Requirements	23
3.1.7 IT Security Audits	24
3.1.7.1 Purpose	24
3.1.7.2 Requirements	24
3.2 IT Contingency Planning	24
3.2.1 Purpose	24
3.2.2 Continuity of Operations Planning	24
3.2.2.1 Purpose	24
3.2.2.2. Requirements	25
3.2.3 IT Disaster Recovery Planning	25
3.2.3.1 Purpose	25
3.2.3.2 Requirements	26
3.2.4 IT System and Data Backup and Restoration	26
3.2.4.1 Purpose	26
3.2.4.2 Requirements	26
3.3 IT Systems Security	27
3.3.1 Purpose	27
3.3.2 IT System Security Plans	27
3.3.2.1 Purpose	27
3.3.2.2 Requirements	28
3.3.3 IT System Hardening	28
3.3.3.1 Purpose	28
3.3.3.2 Requirements	28
3.3.3.3 System Security Testing Tools	29
3.3.4 IT Systems Interoperability Security	30
3.3.4.1 Purpose	30
3.3.4.2 Requirements	30
3.3.5 Malicious Code Protection	31
3.3.5.1 Purpose	31
3.3.5.2 Requirements	31
3.3.6 IT Systems Development Life Cycle	32
3.3.6.1 Purpose	32
3.3.6.2 Requirements	32
3.3.7 Application Security	34
3.3.7.1 Purpose	34
3.3.7.2 Requirements	34
3.4 Logical Access Control	36
3.4.1 Purpose	36
3.4.2 Account Management	36
3.4.2.1 Purpose	36
3.4.2.2 Requirements	37
3.4.3 Password Management	39
3.4.3.1 Purpose	39
3.4.3.2 Requirements	39
3.4.4 Remote Access	41
3.4.4.1 Purpose	41
3.4.4.2 Requirements	41
3.5 Data Protection	42
3.5.1 Purpose	42
3.5.2 Data Storage Media Protection	42
3.5.2.1 Purpose	42
3.5.2.2 Requirements	42
3.5.3 Encryption	44

3.5.3.1 Purpose	44
3.5.3.2 Policy	44
3.5.3.3 Requirements	44
3.6 Facilities Security	45
3.6.1 Purpose	45
3.6.2 Policy	45
3.6.3 General Facilities Security	45
3.6.4 IT Facilities Security	45
3.7 Personnel Security	46
3.7.1 Purpose	46
3.7.2 Access Determination and Control	46
3.7.2.1 Purpose	46
3.7.2.2 Requirements	46
3.7.3 IT Security Awareness and Training	47
3.7.3.1 Purpose	47
3.7.3.2 Requirements	48
3.7.4 Acceptable Use	49
3.7.4.1 Purpose	49
3.7.4.2 Requirements	49
3.7.5 Email Communication	53
3.7.5.1 Purpose	53
3.7.5.2 Email Disclosure Requirements	53
3.8 Threat Management	54
3.8.1 Purpose	54
3.8.2 Threat Detection	54
3.8.2.1 Purpose	54
3.8.2.2 Requirements	54
3.8.3 IT Security Monitoring and Logging	55
3.8.3.1 Purpose	55
3.8.3.2 Requirements	55
3.8.4 IT Security Incident Handling	56
3.8.4.1 Purpose	56
3.8.4.2 Definitions	56
3.8.4.3 MS-ISAC Keylogging Reports	57
3.8.4.4 Requirements	57
3.8.5 Data Breach Notification	62
3.8.5.1 Purpose	62
3.8.5.2 Requirements	62
3.9 IT Asset Management	64
3.9.1 Purpose	64
3.9.2 IT Asset Control	65
3.9.2.1 Purpose	65
3.9.2.2 Requirements	65
3.9.3 Software License Management	66
3.9.3.1 Purpose	66
3.9.3.2 Requirements	66
3.9.4 Configuration Management and Change Control	66
3.9.4.1 Purpose	66
3.9.4.2 Requirements	66
3.10 Additional Security Requirements in Third-Party Contracts	67
3.10.1 Purpose	67
3.10.2 Requirements	67

3.11 Collection of Evidence	68
3.11.1 Purpose	68
3.11.2 Requirements	68
3.12 Additional Requirements for Protecting COV Data	69
3.12.1 Purpose	69
3.12.2 Requirements	69
3.13 Additional Requirements for Protecting COV Data when Using Telephones	70
3.13.1 Purpose	70
3.13.2 Requirements	70
<i>4.0 Information Security Terms and Concepts.....</i>	<i>71</i>
<i>5.0 Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media</i>	<i>74</i>

Approval

		
Douglas G. Mack IT Security Director ISO	Dave Burhop Assistant Commissioner CIO	D.B. Smit Commissioner Agency Head
2-13-09	2-17-09	2-17-09
Date	Date	Date

Revision History

Version	Date	Purpose of Revision
1.0	07/25/08	Base Document
1.1	07/29/08	Beginning changes and additions
1.2	09/08/08	Draft 1 – Given to IA for Review
1.3	10/15/08	Draft 2 – Incorporates Changes from IA
1.4	10/31/08	Draft 2 – Given to CIO for Review
1.5	12/30/08	Draft 3 – Incorporates Changes from CIO
1.6	01/09/09	Sent to Commissioner through CIO
1.7	02/13/09	APPROVED VERSION

1.0 Introduction

1.1 Overview

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 Technology Security (“IT Security”) Policy. The agency IT Security Policy is intended to protect the confidentiality, integrity, and availability of electronic information.

DMV relies on the application of information technology (IT) for the effective delivery of government services. Rapid and continuing technical advances have increased the dependence of DMV on IT. DMV data, software, hardware, and telecommunications are recognized as important resources and must be protected through the agency IT Security Policy.

To be effective, IT security must be a team effort involving the participation and support of every DMV employee. It remains the policy of DMV that each employee is responsible for the security of the agency's data and for taking appropriate steps to secure agency IT systems and data through complying with the agency IT Security Policy as stated in this policy.

1.2 Review

The policies contained herein shall be reviewed annually from the date of final approval by the IT Security Director who will forward a confirmation of said review to the Commissioner, Chief Information Officer (CIO), and Director of Internal Audit.

1.3 Policy/Legal Conflicts

The IT Security Policy for DMV was written to meet or exceed the protections found in existing laws and regulations, and any DMV IT security policy believed to be in conflict with existing laws or regulations must be promptly reported to the IT Security Director.

In the event of a conflict between DMV IT Security Policy and existing laws or regulations, the following is the order of precedence to resolve the conflict:

1. Federal/State law which takes precedence over
2. COV IT Security Policy, Standards, Guidelines which takes precedence over
3. This IT Security Policy which takes precedence over
4. DMV IT Security Policies.

1.4 Exceptions

It is acknowledged that under rare circumstances, it may be necessary to deviate from the policies and standards contained in this document. The IT Security Director, or authorized designee, must approve all such deviations in writing.

In such cases, 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 risk management process requires approval by the System Owner, Data Owner (if applicable), and IT Security Director.

In such cases, when necessary, the procedure for submitting an *IT Security Policy and Standard Exception Request Form* with VITA will be followed.

1.5 Enforcement

Classified employees may be subject to disciplinary action up to and including discharge, under the Commonwealth's Standards of Conduct; and 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.

1.6 Policy Non-Enforcement

DMV's non-enforcement of any policy requirement does not constitute its consent.

1.7 Violation of Law

All known violations of the law shall be immediately reported to DMV Special Investigations Unit (SIU).

1.8 Authority

- *Code of Virginia* § 2.2-603(G) (Authority of Agency Directors)
- *Code of Virginia*, §§ 2.2-2005 – 2.2-2032. (Creation of the Virginia Information Technologies Agency; "VITA;" Appointment of Chief Information Officer (CIO))
- *Code of Virginia*, §2.2-2009 (Additional Powers of the CIO relating to security)
- *Code of Virginia*, §2.2-2457 (Information Technology Investment Board)

- *Code of Virginia*, §2.2-2827 (Restrictions on State employee access to information Infrastructure)
- *Code of Virginia*, §2.2-3803 (Administration of systems including personnel information; Internet privacy policy)
- *Code of Virginia*, §18.2-186.6 (Breach of personal information notification)
- *IT Information Security Policy* (SEC500-02) (07/17/2008)
- *IT Information Security Standard* (SEC501-01) (07/31/2008)
- *IT Security Audit Standard* (SEC502-00) (01/11/2007) (Compliance Date: 02/01/2007)
- *IT Standard Use of Non-Commonwealth Computing Devices to Telework* (SEC511-00) (07/01/2007)
- *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard* (SEC514-03) (03/15/2008)
- *Internet Privacy Guidelines* (SEC2001-02.1) (02/27/2001)
- *IT Contingency Planning Guideline* (SEC508-00) (4/18/07)
- *IT Data Protection Guideline* (SEC507-00) (7/02/07)
- *IT Logical Access Control Guideline* (SEC509-00) (4/18/07)
- *IT Personnel Security Guideline* (SEC513-00) (2/15/2008)
- *IT Risk Management Guideline* (SEC506-01) (12/11/2006)
- *IT Risk Assessment Instructions- Appendix D* (SEC506-01) (12/14/2006)
- *IT Security Audit Guideline* (SEC512-00) (12/20/2007)
- *IT Security Threat Management Guideline* (SEC510-00) (07/01/2007)
- *IT Systems Security Guideline* (SEC515-00) (07/17/2008)

1.9 Freedom of Information (FOIA)

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 from the Department of Motor Vehicles (DMV) is also governed by the Federal Driver's Privacy Protection Act (18 USC §§ [2721 - 2725](#)) and by Va. Code §§ [46.2-208](#) through 214. 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 214 and applicable fees are paid.

2.0 Policy Implementation

2.1 Purpose

This Policy implements the DMV IT Security Policy per the statutory, regulatory, and policy requirements of The Commonwealth. It defines the governance, implementation, roles and responsibilities, standards, guidelines, enforcement, and review of the security policy.

2.2 Scope

This policy applies to the entire Virginia Department of Motor Vehicles including employees, contractors, consultants, and all other personnel with access to DMV Information systems and networks.

2.3 Policy

2.3.1 Goal

There is hereby created an IT Security Policy for DMV.

The goal of the policy is to ensure the confidentiality, integrity, and availability of all DMV information stored, processed, and/or transmitted in electronic form.

At a minimum, the IT Security Policy for DMV will meet the requirements for an IT security Policy per the current COV Policy, Standards, and Guidelines.

2.3.2 IT Security Policy Development and Direction

The IT Security Policy for DMV shall be developed and administered by the IT Security Director under the direction of the Assistant Commissioner/CIO.

The IT Security Director, to the fullest extent of the position's authority, ensures DMV data in all environments is properly secured, and that policies, procedures and standards are enforced for internal and external users.

The IT Security Director does not implement technology or technological alternatives, but directs via policies, standards and guidelines the information policy needed to accomplish DMV security objectives many of which are accomplished through VITA.

2.3.3 Management Security Approach

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 business.

2.3.4 Information Security Resources

The Commissioner shall allocate sufficient resources and staff attention to adequately address information systems security.

2.3.5 Systems Administrators Don't Handle Security Administration

To achieve proper separation of duties, for all DMV production systems, System Administrators shall not attend to, or otherwise be responsible for, information systems security administration.

2.3.6 Disabling Critical Security Components

Critical components of DMV information security infrastructure shall not be disabled, bypassed, turned off, or disconnected without prior approval from the IT Security Director.

2.3.7 Information Security Compliance

Outside consultants, contractors, and temporaries shall be subject to the same information security requirements, and have the same information security responsibilities, as DMV employees.

2.3.8 Effective Date of DMV IT Security Policy

2.3.8.1 Approved by Commissioner

Upon final approval by the Commissioner of this IT Security Policy, it immediately goes into effect as the IT Security Policy for DMV.

2.3.8.2 Exceptions

All policies referred to in this IT Security Policy will be revised and/or written to be in full compliance with this IT Security Policy no later than July 1, 2009.

Said policies will become immediately effective upon approval of the IT Security Director, Assistant Commissioner/CIO, and the Commissioner.

3.0 Policies

3.1 Risk Management

3.1.1 Purpose

Risk Management delineates the steps necessary to identify, analyze, prioritize, and mitigate risks that could compromise IT systems. This section defines requirements in the following areas:

- IT Security Roles and Responsibilities
- Business Impact Analysis
- IT System and Data Sensitivity Classification
- Sensitive IT System Inventory and Definition
- Risk Assessment
- IT Security Audits

3.1.2 IT Security Roles and Responsibilities

3.1.2.1 Purpose

IT Security Roles and Responsibilities requirements identify the steps necessary to establish formal roles and assign responsibilities to manage and protect the security of IT systems.

3.1.2.2 Requirements

1. The Commissioner shall designate an Information Security Officer (ISO) for DMV, and provide the person's name, title (IT Security Director), and contact information to the Commonwealth Chief Information Security Officer (CISO) via email to VITASecurityServices@vita.virginia.gov no less than biennially.
2. The Commissioner shall designate the Assistant Commissioner/CIO as backup for the ISO.
3. The Commissioner shall assign individuals to the roles described in the current version of the *Information Technology Security Policy* (COV ITRM Policy SEC500).
4. The IT Security Director shall document the responsibilities of the designee for each role identified.
5. The IT Security Director shall review System Security Plans for all sensitive agency IT systems and:
 - a. Approve those System Security Plans that provide adequate protections against IT security risks; or
 - b. Disapprove System Security Plans that do not provide adequate protections against IT security risks, and require that the System Owner implement additional security controls on the IT system to provide adequate protections against IT security risks.
6. The Commissioner shall prevent conflict of interests and adhere to the security concept of separation of duties by assigning roles so that:
 - a. The IT Security Director is not a System Owner or a Data Owner except in the case of compliance systems for IT Security;
 - b. The System Owner and the Data Owner are not System Administrators for IT systems or data they own; and
 - c. The IT Security Director, System Owners, and Data Owners are COV employees.

- d. Other roles can be assigned to contractors. For roles assigned to contractors, the contract language shall include specific responsibility and background check requirements.
 - e. The System Owner can own multiple IT systems.
 - f. Data Owners can own data on multiple IT systems.
 - g. System Administrators can assume responsibility for multiple IT systems.
7. The IT Security Director shall review the position descriptions of all employees assigned to IT security roles annually, or more often as necessary, and verify that the position descriptions accurately reflect assigned IT security duties and responsibilities.

3.1.2.3 DMV IT Security Roles

1. Agency Head (DMV Commissioner)

DMV Commissioner is responsible for the security of the agency's IT systems and data. DMV Commissioner's IT security responsibilities include the following:

- a. Designate an ISO for the agency and providing the person's name, title (IT Security Director) and contact information to VITA no less than biennially.
- b. The Agency Head shall designate the Assistant Commissioner/CIO as backup for the ISO, as well.
- c. The IT Security Director (ISO) reports to the Assistant Commissioner, CIO.
- d. Maintain an agency IT security program that is sufficient to protect the agency's IT systems, and that is documented and effectively communicated.
- e. Review and approve the agency's Business Impact Analyses (BIAs), a Risk Assessment (RA), and a Continuity of Operations Plan (COOP), to include an IT Disaster Recovery Plan, if applicable.

- f. Maintain compliance with the current version of the IT Security Audit Standard (COV ITRM Standard SEC502). This compliance must include, but is not limited to:
 - Requiring development and implementation of an agency plan for IT security audits, and submitting this plan to the CISO;
 - Requiring that the planned IT security audits are conducted;
 - Receiving reports of the results of IT security audits;
 - Requiring development of Corrective Action Plans to address findings of IT security audits; and
 - Reporting to the Commonwealth Chief Information Security Officer (CISO) all IT security audit findings and progress in implementing corrective actions in response to IT security audit findings.
- g. Facilitate the communication process between data processing staff and those in other areas of the agency.
- h. Establish a program of IT security safeguards.
- i. Provide the resources to enable employees to carry out their responsibilities for securing IT systems and data.

Managers in all agencies and at all levels shall provide for the IT security needs under their jurisdiction. They shall take all reasonable actions to provide adequate IT security and to escalate problems, requirements, and matters related to IT security to the highest level necessary for resolution.

2. Assistant Commissioner/Chief Information Officer (CIO)

The Assistant Commissioner/CIO is responsible for the management of Information Technology Services (ITS) at DMV.

The Assistant Commissioner/CIO is the direct supervisor of the IT Security Director/ISO.

The Assistant Commissioner/CIO is the designated Backup ISO for DMV.

3. Information Security Officer (ISO) (DMV IT Security Director)

At DMV the title of the ISO is IT Security Director.

The IT Security Director is responsible for developing and managing the DMV's IT security program. Working under the direction of the Assistant Commissioner/CIO, the IT Security Director's duties are as follows:

- a. Develop and manage an agency IT security program that meets or exceeds the requirements of COV IT security policies and standards in a manner commensurate with risk.
- b. Verify and validate that all agency IT systems and data are classified for sensitivity.
- c. Develop and maintain an IT security awareness and training program for agency staff, including contractors and IT service providers.
- d. Coordinate and provide IT security information to the CISO as required.
- e. Implement and maintain the appropriate balance of protective, detective and corrective controls for agency 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.
- g. Maintain liaison with the CISO.

4. System Owner

The System Owner is the DMV manager responsible for operation and maintenance of DMV's IT system. With respect to IT security, the System Owner's responsibilities include the following:

- a. Require that all IT system users complete required IT security awareness and training activities prior to, or as soon as practicable after, receiving access to the system, and no less than annually, thereafter.
- b. Manage system risk and developing any additional IT security policies and procedures required to protect the system in a manner commensurate with risk.
- c. Maintain compliance with COV IT 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.

5. Data Owner

The Data Owner is the DMV manager responsible for the policy and practice decisions regarding data, 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.

6. System Administrator

The System Administrator is an analyst, engineer, or consultant who implements, manages, and/or operates a system or systems at the direction of the System Owner, Data Owner, and/or Data Custodian.

The System Administrator assists agency management in the day-to-day administration of agency IT systems, and implements security controls and other requirements of the agency IT security program on IT systems for which the System Administrator have been assigned responsibility.

7. Data Custodian

Data Custodians are individuals or organizations in physical or logical possession of data for Data Owners. Data Custodians are responsible for the following:

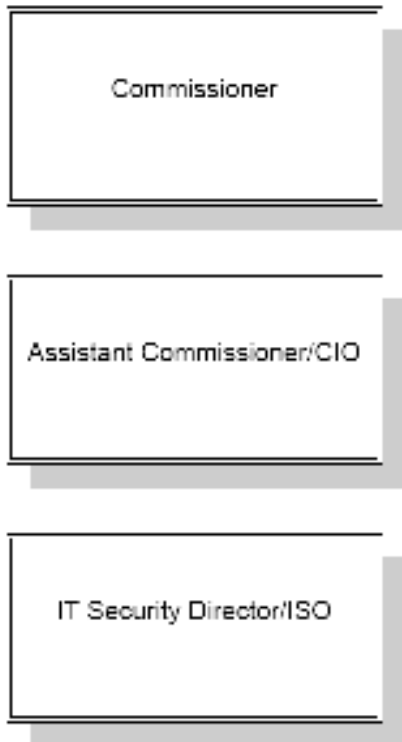
- a. Protect the data in their possession from unauthorized access, alteration, destruction, or usage.
- b. Establish, monitoring, and operating IT systems in a manner consistent with COV IT security policies and standards.
- c. Provide Data Owners with reports, when necessary and applicable.

8. IT System Users

All users of COV IT systems including employees and contractors are responsible for the following:

- a. Read and comply with DMV IT Security Policy requirements.
- b. Report breaches of IT security, actual or suspected, to the IT Security Director and DMV management and/or the CISO.
- c. Take reasonable and prudent steps to protect the security of IT systems and data to which they have access.

9. IT Security Organizational Chart



3.1.3 Business Impact Analysis

3.1.3.1 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.

3.1.3.2 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

3.1.4 IT System and Data Sensitivity Classification

3.1.4.1 Purpose

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.

3.1.4.2 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.
5. Server names and configuration.

3.1.4.3 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 similar to the following table. Data Owners must classify sensitivity requirements of all types of data. The following table is only an illustration.

System ID: ABC123	Sensitivity Criteria		
Type of Data	Confidentiality	Integrity	Availability
HR Policies	Low	High	Moderate
Medical Records	High	High	High
Criminal Records	High	High	High

Table 1: Sample Sensitivity Analysis Results

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.

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.

3.1.5 Sensitive IT System Inventory and Definition

3.1.5.1 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.

3.1.5.2 Requirements

1. The IT Security Director shall document each sensitive IT system owned by the agency, including its ownership and boundaries, and update the documentation as changes occur.

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 for the purposes of this Standard, upon request, the CIO of the Commonwealth will determine the System Owner.

2. The Commissioner, or designee, shall assign a System Owner, Data Owner(s), and System Administrator(s) for each agency-owned sensitive IT system.

Note: A sensitive IT system may have multiple Data Owners, and/or System Administrators, but must have a designated System Owner.

3. The IT Security Director shall maintain or require that its service provider maintain updated network diagrams.

3.1.6 Risk Assessment

3.1.6.1 Purpose

Risk Assessment requirements delineate the steps DMV 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.

Note: The Risk Assessment (RA) required by this Standard differs from the RA required by the current version of the Project Management Standard (COV ITRM Standard GOV2004). This Standard requires an RA based on operational risk, while the Project Management Standard requires an RA based on project risk. Many of the RA techniques described in the Project Management Standard, however, may also be applicable to the RA required by this Standard.

3.1.6.2 Requirements

For each IT system classified as sensitive, the IT Security Director shall:

1. Conduct a formal RA of the IT system, as needed, but not less than once every three years.
2. Conduct an annual self-assessment to determine the continued validity of the formal 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.

3.1.7 IT Security Audits

3.1.7.1 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.”

3.1.7.2 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.

3.2 IT Contingency Planning

3.2.1 Purpose

IT Contingency Planning delineates the steps necessary to plan for and execute recovery and restoration of IT systems and data if an event occurs that renders the IT systems and/or data unavailable. This component of the DMV IT Security Policy defines requirements in the following three areas:

- Continuity of Operations Planning
- Disaster Recovery Planning
- IT System Backup and Restoration

3.2.2 Continuity of Operations Planning

3.2.2.1 Purpose

COV Continuity of Operations Planning requirements are defined by VDEM. This section addresses only the Continuity of Operations Planning requirements for IT systems and data. Agencies should consult the Continuity of Operations Planning Manual published by VDEM for non-IT related requirements that address all essential business functions. The agency’s overall Continuity of Operations Plan (COOP) should include

the manual processing procedures for critical functions that users can follow until the agency restores operations, as appropriate.

These Continuity of Operations Planning requirements identify the steps necessary to provide continuity for essential agency IT systems and data through the development, implementation, exercise, and maintenance of the IT component of Continuity of Operations Plans.

3.2.2.2. Requirements

1. The Commissioner shall designate an employee to collaborate with the agency Continuity of Operations Plan (COOP) coordinator as the focal point for IT aspects of COOP and related Disaster Recovery planning activities.

Note: Designation of an agency COOP coordinator is included in the COOP planning requirements issued by VDEM.

2. The IT Security Director, based on BIA and RA results, shall develop agency COOP IT-related documentation which identifies:
 - a. Essential business functions that require restoration and the Recovery Time Objective (RTO) for each;
 - b. Recovery requirements for IT systems and data needed to support the essential business functions; and
 - c. Personnel contact information and incident notification procedures.

Note: The COOP should be protected as sensitive data and stored at a secure off-site location.

3. The Commissioner shall require an annual exercise (or more often as necessary) of IT COOP components to assess their adequacy and effectiveness.
4. The Commissioner shall require the review and revision of IT COOP components following the exercise (and at other times as necessary).

3.2.3 IT Disaster Recovery Planning

3.2.3.1 Purpose

IT Disaster Recovery Planning is the component of Continuity of Operations Planning that identifies the steps necessary to provide for restoring essential business functions on a schedule that support agency mission requirements. These steps lead to the creation of an IT Disaster Recovery Plan (DRP).

3.2.3.2 Requirements

The IT Security Director:

1. Based on the COOP, develop and maintain an IT DRP, which supports the restoration of essential business functions.
2. Require approval of the IT DRP by the Commissioner or designee.
3. Require periodic review, reassessment, testing, and revision of the IT DRP to reflect changes in essential business functions, services, IT system hardware and software, and personnel.
4. Establish communication methods to support IT system users' local and remote access to IT systems, as necessary.

3.2.4 IT System and Data Backup and Restoration

3.2.4.1 Purpose

IT System and Data Backup and Restoration requirements identify the steps necessary to protect the availability and integrity of COV data documented in backup and restoration plans.

3.2.4.2 Requirements

For every IT system identified as sensitive, the IT Security Director shall, or shall require that its service provider (VITA), implement backup and restoration plans to support restoration of systems and data in accordance with DMV requirements. At a minimum, these plans shall address the following:

1. Secure off-site storage for backup media.
2. Store off-site backup media in an off-site location that is geographically/separate and distinct from the primary location.
3. Performance of backups only by authorized personnel.
4. Review of backup logs after the completion of each backup job to verify successful completion.
5. Approval of backup schedules of a system by the System Owner.

6. Approval of emergency backup and operations restoration plans by the System Owner.
7. Protection of any backup media that is sent off site (physically or electronically), or shipped by the United States Postal Service or any commercial carrier, in accordance with agency requirements.
8. Authorization and logging of deposits and withdrawals of all media that is stored off-site.
9. Retention of the data handled by an IT system in accordance with the agency's records retention policy.
10. Management of electronic information in such a way that it can be produced in a timely and complete manner when necessary, such as during a legal discovery proceeding.

3.3 IT Systems Security

3.3.1 Purpose

IT Systems Security requirements delineate steps to protect IT systems in the following six areas:

- IT System Security Plans
- IT System Hardening
- IT Systems Interoperability Security
- Malicious Code Protection
- IT Systems Development Life Cycle
- Application Security

3.3.2 IT System Security Plans

3.3.2.1 Purpose

IT System Security Plans document the security controls required to demonstrate adequate protection of IT systems against IT security risks.

3.3.2.2 Requirements

Each System Owner of a sensitive IT system shall:

1. Document an IT System Security Plan for the IT system based on the results of the risk assessment. This documentation shall include a description of:
 - a. All IT existing and planned IT security controls for the IT system, including a schedule for implementing planned controls;
 - b. How these controls provide adequate mitigation of risks to which the IT system is subject.
2. Submit the IT System Security Plan to the IT Security Director for approval.
3. Plan and document additional IT security controls for the IT system if the IT Security Director disapproves the IT System Security Plan, and resubmit the IT System Security Plan to the Commissioner or designated ISO for approval.
4. Update the IT System Security Plan every three years, or more often if necessary, and resubmit the IT System Security Plan to the IT Security Director.

3.3.3 IT System Hardening

3.3.3.1 Purpose

IT System Hardening requirements delineate technical security controls to protect IT systems against IT security vulnerabilities.

3.3.3.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA):

1. Ensure that industry-based best practices are utilized to ensure the appropriate technical security controls are implemented and tested.
2. Ensure that all security-related service packs, patches and hot-fixes are tested and applied to all systems in a timely manner and in accordance with DMV's Configuration and Change Management (CCM) process.
3. Ensure that all systems are physically secured.

4. Identify, document, and apply appropriate baseline security configurations to agency IT systems, regardless of their sensitivity.
5. Identify, document, and apply more restrictive security configurations for sensitive agency IT systems, as necessary.
6. Maintain records that document the application of baseline security configurations.
7. Review and revise all security configuration standards annually, or more frequently, as needed.
 - a. The IT Security Director shall or shall require that its service provider (VITA) establish a process to review and catalog applicable security notifications issued by equipment manufacturers, bulletin boards, security-related Web sites, and other security venues, and establish a process to update security baseline configuration standards based on those notifications.
8. Reapply all security configurations to agency-owned IT systems, as appropriate, when the IT system undergoes a material change, such as an operating system upgrade.
9. Require periodic vulnerability scanning of IT systems in a manner commensurate with sensitivity and risk, to verify whether security configurations are in place and if they are functioning effectively.
10. Modify individual IT system configurations or baseline security configuration standards, as appropriate, to improve their effectiveness based on the results of vulnerability scanning.

3.3.3.3 System Security Testing Tools

DMV users, including employees, contractors, 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.

3.3.4 IT Systems Interoperability Security

3.3.4.1 Purpose

IT System Interoperability Security requirements identify steps to protect data shared with other IT systems.

3.3.4.2 Requirements

For every sensitive agency-owned IT system, the IT Security Director shall require or shall specify that its service provider (VITA) require:

1. The System Owner, in consultation with the Data Owner, document IT systems with which data is shared. This documentation shall include:
 - a. The types of shared data;
 - b. The direction(s) of data flow; and
 - c. Contact information for the organization that owns the IT system with which data is shared, including the System Owner, the Information Security Officer (ISO), or equivalent, and the System Administrator.
2. The System Owners of the IT systems which share data develop a written agreement that delineates IT security requirements for each interconnected IT system and for each type of data shared.
3. The System Owners of the IT systems that share data inform one another regarding other IT systems with which their IT systems interconnect or share data, and inform one another prior to establishing any additional interconnections or data sharing.
4. The written agreement specify if and how the shared data will be stored on each IT system.
5. The written agreement specify that System Owners of the IT systems that share data acknowledge and agree to abide with any legal requirements (i.e., HIPAA) regarding handling, protection, and disclosure of the shared data.
6. The written agreement maintains each Data Owner's authority to approve access to the shared data.
7. The System Owners approve and enforce the agreement.

3.3.5 Malicious Code Protection

3.3.5.1 Purpose

Malicious Code Protection requirements identify controls to protect IT systems from damage caused by malicious code.

3.3.5.2 Requirements

The IT Security Director shall, or shall require that its service provider (VITA):

1. Prohibit all IT system users from intentionally developing or experimenting with malicious programs (e.g., viruses, worms, spy-ware, 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 program detection, protection, eradication, logging, and reporting capabilities.
4. Provide malicious code protection mechanisms on multiple IT systems and for all IT system users preferably deploying malicious code detection products from multiple vendors on various platforms.
5. Require malicious program protection that:
 - a. Eliminates or quarantines malicious programs that it detects;
 - b. Provides an alert notification;
 - c. Automatically and periodically runs scans on memory and storage devices;
 - d. Automatically scans all files retrieved through a network connection, modem connection, or from an input storage device;
 - e. Allows only authorized personnel to modify program settings; and
 - f. Maintains a log of protection activities.
6. Provide the ability to eliminate or quarantine malicious programs in email messages and file attachments as they attempt to enter the agency's email system.
7. Provide the ability for automatic download of definition files for malicious code protection programs whenever new files become available, and propagate the new files to all devices protected by the malicious code protection program.

8. Require all forms of malicious code protection to start automatically upon system boot.
9. Provide network designs that allow malicious code to be detected and removed or quarantined before it can enter and infect a production device.
10. Provide procedures that instruct administrators and IT system users on how to respond to malicious program attacks, including shutdown, restoration, notification, and reporting requirements.
11. Require use of only new media (e.g., diskettes, CD-ROM) or sanitized media for making copies of software for distribution.
12. Prohibit the use of common use workstations and desktops (e.g., training rooms) to create distribution media.
13. By written policy, prohibit the installation of software on agency IT systems until the software is approved by DMV ISO or designee and, where practicable, enforce this prohibition using automated software controls, such as Active Directory security policies.
14. Establish Operating System (OS) update schedules commensurate with sensitivity and risk.

3.3.6 IT Systems Development Life Cycle

3.3.6.1 Purpose

IT Systems Development Life Cycle Security requirements document the security-related activities that must occur in each phase of the development life cycle (from project definition through disposal) for agency-owned IT application systems.

3.3.6.2 Requirements

The IT Security Director shall, or shall require the Systems Development Division to:

1. Incorporate IT security requirements in each phase of the life cycle, as well as for each modification proposed for the IT application system in each stage of its life cycle.

Project Initiation

2. Perform an initial risk analysis based on initial requirements and the business objectives to provide high-level security guidelines for the system developers.
3. Classify the types of data that the IT system will process and the sensitivity of proposed IT system.
4. Assess the need for collection and maintenance of sensitive data before incorporating such collection and maintenance in IT system requirements.
5. Develop an initial IT System Security Plan that documents the IT security controls that the IT system will enforce to provide adequate protection against IT security risks.

Project Definition

6. Identify, develop, and document IT security requirements for the IT system during the Project Definition phase.
7. Incorporate IT security requirements in IT system design specifications.
8. Verify that the IT system development process designs, develops, and implements IT security controls that meet the IT security requirements in the design specifications.
9. Update the initial IT System Security Plan to document the IT security controls included in the design of the IT system to provide adequate protection against IT security risks.
10. Develop IT security evaluation procedures to validate that IT security controls developed for a new IT system are working properly and are effective.

Note: Some IT security controls (primarily those controls of a non-technical nature) cannot be tested and evaluated until after deployment of the IT system.

Implementation

11. Execute the IT security evaluation procedures to validate and verify that the functionality described in the specification is included in the product.

Note: Results should be documented in a report, including identification of controls that did not meet design specifications.

12. Conduct a RA to assess the risk level of the IT application system.
13. Require that the IT system comply with all relevant Risk Management requirements in Section 3.1 of this document.
14. Update the IT System Security Plan to document the IT security controls included in the IT system as implemented to provide adequate protection against IT security risks.

Disposition

15. Require retention of the data handled by an IT system in accordance with the DMV's records retention policy prior to disposing of the IT system.
16. Require that electronic media is sanitized prior to disposal, as documented in Section 3.5.2, so that all data is removed from the IT system.
17. 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).

3.3.7 Application Security

3.3.7.1 Purpose

Application security requirements define the high level specifications for securely developing and deploying Commonwealth applications.

3.3.7.2 Requirements

The IT Security Director is accountable for ensuring the following steps are followed and documented:

Application Planning

1. Data Classification - Data used, processed or stored by the proposed application shall be classified according to the sensitivity of the data.
2. 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.

3. Security Requirements – Identify and document the security requirements of the application early in the development lifecycle. For a sensitive system, this shall be done after a risk assessment is completed and before development begins.
4. Security Design – Use the results of the Data Classification process to assess and finalize any encryption, authentication and access control, and logging requirements.
5. Security shall be addressed at all life cycle stages of the software development lifecycle (SDLC).

Application Development

The following requirements represent a minimal set of coding practices, which shall be applied to all applications that utilize un-trusted data.

6. Input Validation – Validate input from all sources. Input validation to be tested should always consider expected and unexpected input, and not block input based on arbitrary criteria.
7. Default deny – Access control should be based on specific permission rather than exclusion. By default all access should be denied.
8. Principle of Least Privilege – All processes should be performed with the least set of privileges required to complete the process.
9. Quality Assurance – Quality assurance is one of the single most effective means of identifying and eliminating software vulnerabilities. Internal testing shall include at least one of the following: penetration testing, fuzz testing, or source code auditing. External source code auditing and/or penetration testing shall be conducted commensurate with sensitivity and risk.

Note: Source code auditing techniques include:

- a. Manual code review can identify vulnerabilities as well as functional flaws, but most companies do not have the skilled security resources or time available within the software lifecycle that a manual code review requires, and therefore many companies who decide to perform manual code reviews can only analyze a small portion of their applications.
- b. Application penetration testing tries to identify vulnerabilities in software by launching as many known attack techniques as possible on likely access points in an attempt to bring down the application or the entire system.
- c. Automated source code analysis tools make the process of manual code review more efficient, affordable, and achievable. This technique of code audit results in significant reduction of analysis time, actionable metrics,

significant cost savings, and can be integrated into all points of the development life cycle.

Production and Maintenance

10. Applications shall be hosted on servers compliant with the Commonwealth Security requirements for IT system hardening (Section 3.3.3).

Applications classified as sensitive shall at a minimum have annual vulnerability assessments run against the applications and supporting server infrastructure and when any significant change to the environment or application has been made. More frequent vulnerability assessments may be done commensurate with sensitivity and risk.

3.4 Logical Access Control

3.4.1 Purpose

Logical Access Control requirements delineate the steps necessary to protect IT systems and data by verifying and validating that users are who they say they are and that they are permitted to use the IT systems and data they are attempting to access.

Users are accountable for any activity on the system performed with the use of their account. This component of the DMV IT Security Policy defines requirements in the following three areas:

- Account Management
- Password Management
- Remote Access

3.4.2 Account Management

3.4.2.1 Purpose

Account Management requirements identify those steps necessary to formalize the process of requesting, granting, administering, and terminating accounts. The IT Security Director shall apply these Account Management practices to all accounts on IT systems, including accounts used by vendors and third parties.

The requirements below distinguish between internal and customer-facing IT systems. Internal IT systems are designed and intended for use only by COV employees, contractors, and business partners; customer-facing IT systems are designed and intended

for use by agency customers and by members of the public. COV employees, contractors, and business partners may also use customer-facing IT systems.

3.4.2.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document formal account management practices for requesting, granting, administering, and terminating accounts. At a minimum, these practices shall include the following components:

For all internal and customer-facing IT systems:

1. Grant IT system users' access to IT systems and data based on the principle of least privilege.
2. Define authentication and authorization requirements, based on sensitivity and risk.
3. Establish policies and procedures for approving and terminating authorization to IT systems.
4. Require requests for and approvals of emergency or temporary access to all sensitive IT systems that:
 - a. Are documented according to standard practice and maintained on file;
 - b. Include access attributes for the account.
 - c. Are approved by the System Owner and communicated to the ISO; and
 - d. Expire after a predetermined period, based on sensitivity and risk.
5. Based on risk, consider use of second-factor authentication, such as tokens and biometrics, for access to sensitive IT systems.
6. Provide for, review at a consistent frequency, relative to sensitivity and risk, of all user accounts for all IT systems to assess the continued need for the accounts.
7. Notify the System Administrator when IT system user accounts are no longer required, or when an IT system user's access level requirements change.
8. Prohibit the use of guest and shared accounts on sensitive IT systems..
9. Prohibit the displaying of user's last name in the logon screen.
10. Lock an account automatically if it is not used for a predefined period.
11. Disable unneeded accounts.

12. Retain unneeded accounts in a disabled state in accordance with the agency's records retention policy.
13. Configure applications to clear cached data and temporary files upon exit of the application or logoff of the system.
14. Associate access levels with group membership, where practicable, and require that every IT system user account be a member of at least one user group.
15. Require that the System Owner and the System Administrator investigate any unusual IT system access activities and approve changes to access level authorizations.
16. Require that System Administrators have both an administrative account and at least one user account and require that administrators use their administrative accounts only when performing tasks that require administrative privileges.
17. Require that local administrator rights, or the equivalent on non-Microsoft Windows-based IT systems, be granted only to authorized IT staff.
18. Require that at least two individuals have administrative accounts to each IT system, to provide continuity of operations.

For all internal and customer-facing IT systems:

19. Require a documented request from the user to establish an account on any internal IT system.
20. Complete any agency-required background check before establishing accounts, or as soon as practicable thereafter.
21. Require employee job descriptions that accurately reflect assigned duties and responsibilities in order to define required IT system access.
22. Require confirmation of the account request and approval by the IT system user's supervisor and approval by the System Owner to establish accounts for sensitive IT systems.
23. Require delivery of access credentials to the user based on information already on file.
24. Notify supervisors, Human Resources, and the System Administrator in a timely manner about termination, transfer of employees and contractors with access rights to internal IT systems and data.

For customer-facing IT systems:

25. Require secure delivery of access credentials to users of all customer-facing IT systems.
26. Require confirmation of the user's request for access credentials based on information already on file prior to delivery of the access credentials to users of sensitive, customer-facing IT systems.
27. Require delivery of access credentials to users of customer-facing sensitive IT systems by means of an alternate channel (i.e., U.S. Mail).

3.4.3 Password Management

3.4.3.1 Purpose

Password Management requirements specify the means for password use to protect IT systems and data.

3.4.3.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document formal password management practices. At a minimum, these practices shall include the following components:

[Note: Effective September 1, 2008, these requirements are being implemented for access to the LAN. DMV is currently working towards implementation of the requirements for other access, such as UNIX and GroupWise.]

1. Require the use of non-shared and a unique password on all accounts on IT systems classified as sensitive, including local, remote access and temporary accounts.
2. Require the use of different passwords on each of the systems to which a user has been granted access.
3. Require passwords on mobile devices issued by the agency such as PDAs and smart phones. For mobile phones, use a 4 to 5 digit pin number.

4. Require password complexity
 - a. at least nine characters in length,
 - b. not be based on a single dictionary word (ex. Bad Password: P4\$sw0rD vs. Good Password: t0YtR4p!), and utilize at least three of the following four:
 - i. Lowercase alpha (e.g. abc)
 - ii. Uppercase alpha (e.g. ABC)
 - iii. Numeric (e.g. 123)
 - iv. Special/Non-Alphanumeric characters (e.g. ! \$ # %)
5. Require that default passwords be changed immediately after installation.
6. Prohibit the transmission of identification and authentication data (e.g., passwords) without the use of industry accepted encryption standards.
7. Require IT system users to maintain exclusive control and use of their passwords, to protect them from inadvertent disclosure to others.
8. Configure sensitive IT systems to allow users to change their password at will.
9. Require users of sensitive IT systems to include network systems to change their passwords after a period of 42 days.
10. Require that IT system users immediately change their passwords and notify the IT Security Director if they suspect their passwords have been compromised.
11. 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.
12. There shall be only three (3) invalid login attempts before the account is locked.
13. Provide a unique initial password for each new user of sensitive IT systems, deliver the initial password to the IT system user in a secure and confidential manner, and require that the IT system user change the initial password upon the first login attempt.
14. Require that forgotten initial passwords be replaced rather than reissued.
15. Prohibit group account IDs and shared passwords on sensitive IT systems.
16. Prohibit the storage of passwords in clear text.

17. Limit access to files containing passwords to the IT system and its administrators.
18. Suppress the display of passwords on the screen as they are entered.
19. Implement a screen saver lockout period after a maximum of 30 minutes of inactivity for COV devices.

COV devices with access to sensitive systems or those devices in less physically secure environments must have a lower time out interval documented and enforced. The lockout period for these systems is after a maximum of 15 minutes of inactivity for COV devices.

20. Determine requirements for hardware passwords based on sensitivity and risk
21. Document and store hardware passwords securely.
22. Implement procedures to handle lost or compromised passwords and/or tokens.

3.4.4 Remote Access

3.4.4.1 Purpose

Information Technology Services (ITS) shall provide remote access to DMV systems by employees and other agency approved personnel when necessary to perform their jobs from a remote location.

Remote Access requirements identify the steps necessary to provide for the secure use of remote access within the COV enterprise network.

3.4.4.2 Requirements

Commensurate with sensitivity and risk, the IT Security Director shall or shall require that its service provider (VITA):

1. Protect the security of all remote access to the agency's sensitive IT systems and data by means of encryption, in a manner consistent with Section 3.5.3.

Note: This encryption requirement applies both to session initiation (i.e., identification and authentication) and to all exchanges containing sensitive data.

2. Protect the security of remote file transfer of sensitive data to and from COV IT systems by means of encryption, in a manner consistent with Section 3.5.3.

3. Document requirements for use of remote access and for remote access to sensitive data, based on DMV and COV policies, standards, guidelines, and procedures.
4. Require that IT system users obtain formal authorization and a unique user ID and password prior to using the agency's remote access capabilities.
5. Document requirements for the physical and logical hardening of remote access devices.
6. Require maintenance of auditable records of all remote access.

3.5 Data Protection

3.5.1 Purpose

Data Protection requirements delineate the steps necessary to protect COV data from improper or unauthorized disclosure. This component of the DMV IT Security Policy defines requirements in the following two areas:

- Data Storage Media Protection
- Encryption

3.5.2 Data Storage Media Protection

3.5.2.1 Purpose

Data Storage Media Protection requirements identify the steps necessary for the appropriate handling of stored data to protect the data from compromise.

3.5.2.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document Data Storage Media protection practices. At a minimum, these practices must include the following components:

1. Define protection of stored sensitive data as the responsibility of the Data Owner.
2. Prohibit the storage of sensitive data on any non-network storage device or media, except for backup media, unless the data is encrypted and there is a written exception approved by the Commissioner that includes the following elements:
 - a. The business or technical justification;
 - b. The scope, including quantification and duration (not to exceed one year);

- c. A description of all associated risks;
- d. Identification of controls to mitigate the risks, one of which must be encryption; and
- e. Identification of any unmitigated risks.

Note: Non-network storage device or media, includes removable data storage media and the fixed disk drives of all desktops and mobile workstations, such as laptop and tablet computers, USB drives, CDs, etc.

Note: A copy of the *Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media* form can be found in section 5.0 of this policy.

3. Require logical and physical protection for all data storage media containing sensitive data, commensurate with sensitivity and risk.
4. Prohibit the connection of any non-COV owned data storage media or device to a COV-owned network, unless the connection is to a segmented guest network. This prohibition, at DMV's discretion, need not apply to an approved vendor providing operational IT support services under contract.

Note: Such media include, but are not limited to, USB drives, cell phones, personal digital assistants, desktops, laptops, and digital music players owned by employees, contractors, and students.

5. Prohibit the auto forwarding of emails to external accounts to prevent data leakage unless there is a documented business case disclosing unmitigated risk approved in writing by the Commissioner.
6. Restrict the pickup, receipt, transfer, and delivery of all data storage media containing sensitive data to authorized personnel.
7. Procedures must be implemented and documented to safeguard handling of all backup media containing sensitive data. Encryption of backup media shall be considered where the data is Personal Health Information (PHI), Personally Identifiable Information (PII), or Critical Infrastructure Information/Sensitive Security Information (CII/SSI). Where encryption is not a viable option, mitigating controls and procedures must be implemented and documented.
8. Implement processes to sanitize data storage media prior to disposal or reuse.

Note: The IT Security Director shall implement procedures to instruct Administrators and users on the disposal of data storage media when no longer needed 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).

3.5.3 Encryption

3.5.3.1 Purpose

Encryption requirements provide a framework for selecting and implementing encryption controls to protect sensitive.

3.5.3.2 Policy

The following policy statements are hereby enacted for DMV:

1. All products that implement encryption must be validated by the National Institute of Standards and Technology (“NIST”) under its Cryptographic Module Validation Program (“CMVP”).
2. Only algorithms approved by NIST under the CMVP are approved for use to protect DMV data.
3. Encryption keys shall be retained for a period of time such that the decrypted data can be retrieved to comply with Virginia FOIA and Library of Virginia requirements.

3.5.3.3 Requirements

Commensurate with sensitivity and risk, the IT Security Director shall:

1. Define and document agency practices for selecting and deploying encryption technologies and for the encryption of data.
2. Document appropriate processes before implementing encryption. These processes must include the following components:
 - a. Instructions in the agency’s IT Security Incident Response Plan on how to respond when keys are compromised;
 - b. A secure key management system for the administration and distribution of encryption keys; and
 - c. Requirements to generate all encryption keys through an approved encryption package and securely store the keys in the event of key loss due to unexpected circumstances.
3. Require encryption during transmission of data that is sensitive relative to confidentiality and integrity.

3.6 Facilities Security

3.6.1 Purpose

Facilities Security requirements identify the steps necessary to safeguard the physical facilities that house IT equipment, systems, services, and personnel.

3.6.2 Policy

It is the policy of DMV that only employees or other authorized persons shall be permitted access to non-public areas of DNV facilities.

3.6.3 General Facilities Security

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>

3.6.4 IT Facilities Security

Successful IT security protection will dictate the physical control of restricted space that contains computer and telecommunications resources.

The following restrictions apply to IT facilities/areas at DMV:

1. Physical access to IT restricted space is based on the principle of least privilege wherein only individuals with a business need for access to restricted space is authorized.
2. IT restricted space is managed by designated employee(s).
3. New and/or planned specifications for IT restricted spaces contain a requirement that the issue of physical security will be coordinated with the IT Security Director during the design phase.
4. The IT Security Director shall perform annual reviews to ensure IT restricted space complies with the policies set in this policy.
5. When possible, entrances to IT restricted space are electronically controlled with the capability of providing an audit trail.
6. The IT Security Director shall periodically review the list of persons allowed physical access to IT restricted space.

7. Any employee or contractor that no longer has a business need to enter IT restricted space will have their access immediately removed.
8. 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.
9. 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.

3.7 Personnel Security

3.7.1 Purpose

Personnel Security requirements delineate the steps necessary to restrict access to IT systems and data to those individuals who require such access as part of their job duties. This component of the DMV IT Security Policy defines requirements in the following three areas:

- Access Determination and Control
- IT Security Awareness and Training
- Acceptable Use
- Email Communication

3.7.2 Access Determination and Control

3.7.2.1 Purpose

Access Determination and Control requirements identify the steps necessary to restrict access to IT systems and data to authorized individuals.

3.7.2.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document access determination and control practices for all sensitive agency IT systems and all third-party IT systems with which sensitive agency IT systems interconnect. At a minimum, these practices shall include the following components:

1. Perform background investigations of all internal IT System users based on access to sensitive IT systems or data. Existing users may be grandfathered under the policy and may not be required to have background investigations.

Note: Agencies should consult the *Code of Virginia* § 2.2-1201.1 and Department of Human Resource Management (DHRM) Policy 2.10.

2. Restrict visitor access to facilities that house sensitive IT systems or data.
3. Require non-disclosure and security agreements for access to IT systems and data, based on sensitivity and risk.
4. Remove physical and logical access rights upon personnel transfer or termination, or when requirements for access no longer exist.
5. Establish termination and transfer practices that require return of agency logical and physical assets that provide access to sensitive IT systems and data and the facilities that house them.
6. Temporarily disable physical and logical access rights when personnel are not working for a prolonged period in excess of 30 days due to leave, disability or other authorized purpose.
7. Disable physical and logical access rights upon suspension of personnel for greater than 1 day for disciplinary purposes.
8. Establish separation of duties in order to protect sensitive IT systems and data, or establish compensating controls when constraints or limitations of DMV prohibit a complete separation of duties.

Example: Such compensating controls may include increased supervisory review; reduced span of control; rotation of assignments; independent review, monitoring, and/or auditing; and timed and specific access authorization with audit review, among others.

9. Explicitly grant physical and logical access to sensitive IT systems and data and the facilities that house them based on the principle of least privilege.

3.7.3 IT Security Awareness and Training

3.7.3.1 Purpose

Security Awareness and Training requirements identify the steps necessary to provide IT system managers, administrators, and users with awareness of system security requirements and of their responsibilities to protect IT systems and data.

3.7.3.2 Requirements

1. The IT Security Director, or staff appointed by him/her, is responsible for all aspects of DMV's security awareness and training program including development, implementation, testing, training, monitoring attendance, and periodic updates.
2. The IT Security Director, or staff appointed by him/her, is responsible for ensuring that DMV-specific IT security training requirements are included in DMV's IT security awareness and training program. An example of such requirements would be those related to accessing DMV customers' records.
3. All DMV IT system users, including employees and contractors, shall be required to complete IT security awareness training annually, or more often as necessary.
4. All DMV IT staff shall be required to complete additional, role-based IT security training annually, or more often as necessary.
5. The IT Security Director, or staff appointed by him/her, is responsible for ensuring that processes to monitor and track completion of IT security awareness training are implemented.
6. DMV IT system users shall be required to complete assigned IT security awareness training no later than 30 days after starting employment at DMV in order to receive and maintain assigned access rights.
7. The IT security awareness training program will be developed so that each IT system user is aware of and understands the following concepts:
 - a. DMV's policy for protecting IT systems and data, with a particular emphasis on sensitive IT systems and data;
 - b. The concept of separation of duties;
 - c. Prevention and detection of IT security incidents, including those caused by malicious code;
 - d. Proper disposal of data storage media;
 - e. Access controls, including creating and changing passwords and the need to keep them confidential;
 - f. DMV acceptable use policies;
 - g. DMV Remote Access policies; and
 - h. Intellectual property rights, including software licensing and copyright issues.
8. Documentation of DMV IT system users' acceptance of DMV's security policies after receiving IT security training.

9. Specialized IT security training for DMV employees, contractors, vendors, business partners, and third parties with specific IT security duties beyond those of all IT systems users is required as practical and necessary. The is would include:
 - a. System Owners, Data Owners, and System Administrator;
 - b. IT Disaster Recovery team members; and
 - c. IT Security Incident Response Team members.

3.7.4 Acceptable Use

3.7.4.1 Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of COV IT systems.

3.7.4.2 Requirements

The IT Security Director shall ensure that these requirements are fully implemented and enforced.

1. All DMV IT users will abide by the Department of Human Resource Management (DHRM) Policy 1.75, “Use of Internet and Electronic Communication Systems.”
2. DMV IT resources are the property of the Commonwealth, or its contracted agents, and are provided for the purpose of transacting official obligations and responsibilities.
3. Limited – incidental or occasional – personal use of DMV IT resources – i.e. non work related – is permitted if:
 - a. It does not adversely affect the performance of official business and duties;
 - b. It does not put COV IT resources to uses that would reflect adversely on the Commonwealth of Virginia to include activities that are illegal, inappropriate, or offensive to fellow employees, contractors, or the public.
4. DMV blocks specific categories of web sites and certain specific web sites for one or more of three reasons:
 - a. Legal Risk – To ensure compliance with applicable Federal/State laws, policies, standards, and guidelines;
 - b. Security Risk – To protect Commonwealth IT assets from malware;

- c. Bandwidth Risk – To ensure adequate bandwidth for agency required processes.

Very often more than one of the reasons is involved with the determination to block a category or web site.

DMV may, at any time, without notice, update the list of prohibited web sites.

- 5. Games may not be stored or used on any DMV computer or computer system.
- 6. The following statements, although not inclusive, define specific unacceptable uses of COV IT resources:
 - a. Accessing, downloading, printing, or storing sexually explicit material in violation of the *Code of Virginia*, §2.2-2827.
 - b. Gambling.
 - c. Use for private or personal gain.
 - d. Use for illegal purpose or any communication that violates applicable laws and regulations.
 - e. Use for product advertisement.
 - f. To transmit threatening, obscene or harassing materials.
 - g. Unauthorized attempts to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.
 - h. Tampering with or otherwise attempting to circumvent security controls.
 - i. Installing or using proprietary encryption hardware/software.
 - j. Interfering with or disrupting network users, services, or equipment. Disruptions include, but are not limited to, distribution of unsolicited advertising, intentional propagation of computer viruses, and using the network to gain unauthorized entry to any other machine accessible through the networks.
 - k. Knowingly uploading or downloading commercial software in violation of its copyright and/or licensing agreement.
 - l. Adding hardware to, removing hardware from, or modifying hardware on a COV system.
 - m. Connecting non-COV-owned devices such as personal computers, laptops, flash devices or hand held devices to a COV IT system or network, except in accordance with the *COV IT Standard Use of Non-Commonwealth Computing Devices to Telework* (SEC511-00).
 - n. Sending large numbers of messages to an individual or a group – i.e. Mail Bombing.
 - o. Attempting to subscribe anyone else to mailing lists.
 - p. Downloading or installing without the authorization of IT Security Director:
 - i. Copyrighted materials.
 - ii. Games.
 - iii. Screen Savers.

- iv. Peer-to-Peer file-sharing programs.
 - v. Non-DMV supported software.
 - q. Playing online electronic games.
 - r. Using unauthorized instant messaging – including, but not limited to, AOL Instant Messenger, Yahoo Instant Messenger, ICQ, Microsoft, etc.
 - s. Using peer-to-peer file sharing applications such as, but not limited to, Gnutella, KaZaA, Musiccity.com, BearShare, LimeWire, XoloX, Auto galaxy, Direct Connect, Toad, Noad, WinMx, Napigator, Morpheus, CuteMx, Scour Exchange, FreeNetfile, eDonkey, and iMesh.
 - t. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
 - u. Posting COV information to external newsgroups, bulletin boards or other public forums without authorization from the IT Security Director.
7. All DMV IT resources use – including but not limited to: Internet use, email, DMV system access – is subject to continuous monitoring and users have no expectation of privacy in regards to any message, file, e-mail, image, or data created, sent, retrieved, or received when using COV owned or maintained computer equipment or access.
8. The Commonwealth of Virginia (COV), in the *Information Technology Security Standard* (SEC501-01, 5.2.2, #17), explicitly prohibits users, with the exception of authorized Information Technology (IT) staff, from having Local Administrator Rights on their computers.
When a user has Local Administrator Rights on his or her computer, he or she is able to install/delete software and change configuration settings - including security settings.

If a user believes he or she has a business need to have Local Administrator Rights to his or her computer, the following procedure must be followed.

a. IT Staff

As authorized IT staff is permitted to have Local Administrator Rights; the exception process is:

The user will provide the IT Security Director with an explanation in writing of the need for Local Administrator Rights for his review. The IT Security Director, with consultation as needed, will then approve or disapprove the request and notify the requestor.

b. Non-IT Staff

An exception to the IT Security Standard will require the approval of the Chief Information Security Officer (CISO) of the Commonwealth.

This can only be obtained by completing the *COV IT Security Policy & Standard Exception Request Form* – which must be signed by the Commissioner – and forwarding it to VITA Security Services.

The user's supervisor will provide the IT Security Director with an explanation in writing of the need for Local Administrator Rights for his review. The IT Security Director, with consultation as needed, will then approve or disapprove the request.

DMV ISO will complete the *COV IT Security Policy & Standard Exception Request Form*, attach his recommendation and notes, and forward it to the CIO (Assistant Commissioner, Information Technology Services) for his review and approval.

The CIO will then approve or disapprove the request and forward/not forward the request to the Commissioner for his review and approval.

The Commissioner will then approve or disapprove the request – requesting information from ITS as needed. The Commissioner will return the request with his approval/disapproval to the IT Security Director.

If the request has been approved by the Commissioner, the IT Security Director will forward it to the CISO for review and approval/disapproval.

The CISO will review, approve or disapprove the request, and return it to the IT Security Director – who will then notify all appropriate individuals.

The list of individuals at DMV authorized to have Local Administrator Rights shall be maintained by DMV ISO.

9. The use of copyrighted and licensed materials on COV systems, unless the COV owns the materials or COV has otherwise complied with intellectual property laws governing the materials, is prohibited.
10. Transmission of unencrypted sensitive data over the Internet is prohibited.
11. Documentation of DMV IT users' acceptance of DMV's Acceptable Use Policy shall be required before or as soon as practicable after, gaining access to DMV IT systems.

3.7.5 Email Communication

3.7.5.1 Purpose

Email shall not be used to send sensitive data unless there is encryption. Encryption is required for the transmission of data that is sensitive relative to confidentiality and integrity.

The IT Security Director shall consider and plan for the issue of DMV email being intercepted, incorrectly addressed, or infected with a virus.

An email disclaimer is a set of statements that are either pre-pended or appended to emails. These statements are frequently used to create awareness of how to treat the data in the email. An email disclaimer is not a substitute for judgment on what content to put into an email.

3.7.5.2 Email Disclosure Requirements

Emails sent from Commonwealth systems are public records of the Commonwealth of Virginia and must be managed as such.

The following is the approved email disclaimer for DMV. Other email disclaimers are prohibited unless the Commissioner issues an approval in writing.

The times it is required to use this disclaimer is still under discussion, as well as a means of automatically adding it to emails.

The information in this email and any attachments may be confidential and privileged. Access to this email by anyone other than the intended addressee is unauthorized. If you are not the intended recipient (or the employee or agent responsible for delivering this information to the intended recipient) please notify the sender by reply email and immediately delete this email and any copies from our computer and/or storage system. The sender does not authorize the use, distribution, disclosure or reproduction of this email (or any part of its contents) by anyone other than the intended recipient(s).

No representation is made that this email and any attachments are free of viruses. Virus scanning is recommended and is the responsibility of the recipient.

3.8 Threat Management

3.8.1 Purpose

Threat Management delineates the steps necessary to protect IT systems and data by preparing for and responding to IT security incidents. This component of the DMV IT Security Policy defines requirements in the following four areas:

- Threat Detection
- IT Security Monitoring and Logging
- IT Security Incident Handling
- Data Breach Notification

3.8.2 Threat Detection

3.8.2.1 Purpose

Threat Detection requirements identify the practices for implementing intrusion detection and prevention.

3.8.2.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document threat detection practices that include the following components, at a minimum:

1. The IT Security Director shall designate an individual to be responsible for DMV's threat detection program, including planning, development, acquisition, implementation, testing, training, and maintenance.
2. The IT Security Director shall ensure that its service provider (VITA) designates individuals to daily review the Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) logs – reporting any abnormalities immediately to the IT Security Director.
3. DMV's service provider (VITA) shall develop and implement, after review and approval of the IT Security Director, required mitigation measures based on the results of IDS and IPS log reviews.
4. The IT Security Director shall maintain regular communication with VITA Security Services and security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

5. DMV's service provider (VITA) shall maintain regular communication with VITA Security Services and security research and coordination organizations, such as US CERT, to obtain information about new attack types, vulnerabilities, and mitigation measures.

3.8.3 IT Security Monitoring and Logging

3.8.3.1 Purpose

IT Security Monitoring and Logging requirements identify the steps necessary to monitor and record IT system activity.

3.8.3.2 Requirements

Commensurate with sensitivity and risk, the IT Security Director shall, or shall require that its service provider (VITA), document IT security monitoring and logging practices that include the following components, at a minimum:

1. The IT Security Director shall ensure that the service provider (VITA) will designate individuals responsible for the development and implementation of IT security logging capabilities, as well as detailed procedures for reviewing and administering the logs.
2. All DMV production application systems that handle sensitive information must generate logs that capture every addition, modification, and deletion to such sensitive information.
3. The IT Security Director shall ensure that the service provider (VITA) will monitor IT system event logs in real time, correlate information with other automated tools, identifying suspicious activities, and provide alert notifications.
4. The service provider (VITA) shall notify, in order of preference, the following individuals of the alerts referenced in number 3 above:
 - a. The IT Security Director, or
 - b. The AITR, or
 - c. The Chief Architect, or
 - d. The SLD.
5. The IT Security Director shall ensure that standards are documented – both DMV and service provider (VITA) – that specify the type of actions that should be taken when a suspicious or apparent malicious activity is taking place. See 3.8.4 *IT Security Handling* below.

6. Keystroke logging is prohibited except when required for security investigations and approved in writing by the Agency Head or for Training Programs.

3.8.4 IT Security Incident Handling

3.8.4.1 Purpose

IT Security Incident Handling requirements identify the steps necessary to respond to suspected or known breaches to IT security safeguards.

3.8.4.2 Definitions

1. An **information security event** is any observable, threatening occurrence to COV information technology infrastructure of data. This includes, but is not limited to, COV systems, services, networks, device, and data housed or transmitted on such technologies.
2. An **information security incident** is an adverse information security event or the threat of the occurrence of such an event.
3. Relevant personnel are aware of the requirements to establish incident identification, declaration, reporting, and handling processes.

Systems/Network Administrators, VCCC Support Personnel, IT Security Director, and VITA Security Services personnel have the authority to declare an IT security incident(s).

4. The following events automatically meet the IT security incident threshold and will be handled and reported as such.
 - a. IDS reports that are re-identified and confirmed as being exploits or compromises that can be confirmed by IDS and/or system logs.
 - b. Direct contact or notification by Virginia or Federal Law Enforcement for either criminal or civil prosecution.
 - c. Complaints from the public about inappropriate activities or attacks.
 - d. US-CERT (Computer emergency Response Team) makes direct contact via telephone or e-mail regarding personnel or an actual exploit, attack, or other anomaly.
 - e. Unauthorized intrusion or damage to a:
 - i. Web site or page;
 - ii. Computer system or network;
 - iii. Wireless access.
 - f. Discovery of the installation and use of unauthorized peer-to-peer software.

- g. Denial of service.
 - h. Unauthorized use of a system or storage of data.
 - i. Unauthorized changes to systems.
 - j. Unauthorized use of chat rooms using the Internet.
 - k. Employee Complaints.
 - l. Unauthorized vulnerability scans.
 - m. Virus infections.
 - n. Suspected theft of DMV/COV equipment.
 - o. Suspected compromise of cryptographic keys.
5. DMV shall have procedures in place addressing how to respond in the event encryption keys are compromised.

3.8.4.3 MS-ISAC Keylogging Reports

1. MS-ISAC Keylogging Reports have a specific handling defined.
2. The Multi-State Information Sharing and Analysis Center (MS-ISAC) provides VITA Security Services with information on U.S. residents, including Virginia residents, whose personal information has been compromised through keylogging software on their home or business computer.
3. VITA Security Services provides DMV IT Security with information on individuals or companies who have access DMV websites and whose personal information has been compromised.
4. The DMV IT Security Analyst reviews the information and obtains additional contact information as need from DMV resources.
5. The DMV IT Security Analyst inserts the required information into Notification Letters that are sent out under the signature of the Assistant Commissioner/CIO.
6. The Notification Letters contain the IT Security Director's contact information to allow the citizen to obtain additional information or answers to any questions they may have.

3.8.4.4 Requirements

The IT Security Director, under the direction of the Assistant Commissioner/CIO, shall document IT security incident handling practices and where appropriate DMV shall incorporate its service provider's (VITA) procedures for incident handling practices that include the following components, at a minimum:

1. The IT Security Director shall designate a Security Incident Response Team (SIRT) to carry out the incident response activities.

The SIRT shall consist of:

- a. The IT Security Director,
 - b. The AITR,
 - c. The Chief Architect,
 - d. The SLD,
 - e. Appropriate technical staff co-opted as necessary,
 - f. Appropriate law-enforcement staff co-opted as necessary,
 - g. Appropriate executive/management staff co-opted as necessary.
2. The IT Security Director is authorized to investigate any suspected or actual incidents that compromise the confidentiality, integrity, or availability of DMV/COV information assets, and to take appropriate action to mitigate the situation.
 3. The IT Security Director shall ensure that the service provider (VITA) identifies and implements controls to deter and defend against cyber attacks to best minimize loss or theft of information and disruption of services.
 4. The IT Security Director shall ensure that the service provider (VITA) implements proactive measures based on cyber attacks to defend against new forms of cyber attacks.
 5. When an information security event occurs or is suspected of occurring, the following information is captured so that the event can be properly classified and prioritized:
 - a. Scope of Incident
Indicate how widespread the incident is. For example, single user, single network, multiple users/networks.
 - b. Impact of Incident
Indicate how the incident has affected IT systems, users, etc. For example: site defacement, denial of service, unauthorized access, etc.
 - c. Information Sensitivity
Indicate the sensitivity of any information affected by the incident. For example, High – Privacy Act data, Medium – COV proprietary but non-sensitive data, Low – Publicly available data.

6. Based on the information collected, the event is evaluated by appropriate incident response personnel (SIRT) and assigned an appropriate priority for work flow routing and reporting.
7. The appropriate incident response personnel (SIRT) verify that the reported event is a security incident using the least intrusive measures in order to preserve forensic evidence.
8. The incident response personnel (SIRT) will identify immediate mitigation procedures, including specific instructions, based on IT security incident categorization level, on whether or not to shut down or disconnect affected IT systems.
 - a. The IT Security Director shall notify the Assistant Commissioner/CIO as soon as possible of any security incident and provide ongoing status reports as needed.
 - i. If the Assistant Commissioner/CIO is not available, the notification will be made to the Commissioner and status reports given to him.
 - b. The IT Security Director will request approval from the Assistant Commissioner/CIO to shut down or disconnect any significant affected IT system.
 - i. “Significant” would generally be anything other than an individual PC.
 - ii. If the Assistant Commissioner/CIO is not available, the approval will be requested from the Commissioner.
9. The IT Security Director shall report IT security incidents to the CISO 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.”
10. The IT Security Director shall establish requirements for internal agency IT security incident recording and reporting requirements, including a template for the incident report.
 - a. When faced with a potential security incident situation, users of DMV systems should:
 - i. Not alter the state of the computer system or continue using it, except as directed to do so by ITS support staff.

- ii. Keep the computer system on and leave all running computer programs as is.
 - iii. Quickly document any messages or strange behaviors the user notices with the system.
 - iv. Report the security incident to VITA/Network Support at (804) – 367 – 6857.
 - v. The user will describe the system problems clearly and calmly so VITA/Network Support personnel can help get the user the correct assistance and support.
- b. VITA/Network Support will obtain as much information from the user as possible and then notify, in order of preference:
 - i. The IT Security Director, or
 - ii. The AITR, or
 - iii. The Chief Architect, or
 - iv. The SLD.
- c. ITS staff who discover a potential security incident will immediately notify, in order of preference, providing them with as much information as possible:
 - i. The IT Security Director, or
 - ii. The AITR, or
 - iii. The Chief Architect, or
 - iv. The SLD.

11. Identification and Coordination

The IT Security Director shall activate the SIRT and ensure these steps are followed:

- a. Identify and assess the evidence in detail;
- b. Maintain a chain of custody;
- c. Control access to the evidence;
- d. Where possible, capture incident information from reports of logs;
- e. If confirmed criminal activity is discovered, immediately notify the appropriate law enforcement;
- f. Confirmed child pornography activity or evidence thereof must be reported to the Federal Bureau of Investigation (FBI) immediately.

12. Containment

During this phase the goal is to limit the scope and magnitude of an incident to keep the incident from getting worse. The IT Security Director shall ensure these

steps are followed:

- a. Deploy the SIRT as needed;
- b. Determine the risk of continuing operations;
- c. Avoid potentially compromised code except as needed to eradicate the problem;
- d. Back up the system, as appropriate, and store backup tapes in a secure location;
- e. Change passwords on compromised systems, where appropriate, and on all systems that regularly interact with the compromised systems.

13. Eradication

During this phase the goal is to eliminate the problem the vulnerabilities that could allow the re-entry of the problem to the system. The IT Security Director shall ensure these steps are followed:

- a. Isolate the incident and determine how it was executed;
- b. Implement appropriate protection techniques such as firewalls and/or router filters, moving the system to a new name/IP address, etc.;
- c. Perform vulnerability analysis;
- d. Remove the cause of the incident;
- e. Locate, if appropriate, the most recent clean back up.

14. Recovery

During this phase the goal is to return the system to a fully operational status. The IT Security Director shall ensure these steps are followed:

- a. Restore the system;
- b. Validate the system. Once the system has been restored, verify that the operation was successful and the system is back to its normal condition. Include DMV application development and systems support group staff where applicable.
- c. Decide when to restore operations. VITA or DMV/ITS management may decide to leave the system offline while operating system upgrades and patches are installed.
- d. Monitor the systems. Once the system is back on line, continue to monitor for back doors that escaped detection.

15. Report IT security incidents only through non-compromised channels.

16. The IT Security Director will ensure that all appropriate levels of management are notified/updated as appropriate.

17. The IT Security Director will ensure that the Commissioner is notified/updated as appropriate.

3.8.5 Data Breach Notification

3.8.5.1 Purpose

To specify the notification requirements for DMV by identifying the triggering factors and necessary responses to unauthorized release of unencrypted sensitive information.

3.8.5.2 Requirements

The IT Security Director shall:

1. Identify all DMV systems, processes, and logical and physical storage locations (whether held by DMV or a third party) that contain Personal Information.

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, when the data elements are neither encrypted nor redacted.

- a. Social Security Number.
- b. Drivers license number or state identification card number issued in lieu of a driver's license number.
- c. Financial account number, or credit card or debit card number, in combination with any required security code, access code, or password that would permit access to a resident's financial accounts.
- d. Other personal identifying information, such as insurance data or date of birth.

“Redact” means alteration or truncation of data such that no more than the following are accessible as part of the information:

- a. Five digits of a social security number; or
- b. The last four digits of a driver's license number, state identification card number, or account number.

Note: The term does not include information that is lawfully obtained from publicly available information or from federal, state, or local government records lawfully made available to the general public.

2. Include provisions in any third party contracts requiring that the third party and third party subcontractors:

- a. Provide immediate notification to DMV of suspected breaches; and
 - b. Allow DMV both to participate in the investigation of incidents and exercise control over decisions regarding external reporting.
3. Provide appropriate notice to affected individuals upon the unauthorized release of unencrypted and/or un-redacted Personal Information by any mechanism, including, but not limited to:
 - a. Theft or loss of digital media including laptops, desktops, tablets, CD's, DVD's, tapes, USB drives, SD cards, etc.
 - b. Theft or loss of physical hardcopy.
 - c. Security compromise of any system.

An individual or entity shall disclose the breach of the security of the system if encrypted information is accessed and acquired in an unencrypted form, or if the security breach involves a person with access to the encryption key.

If a data custodian is the entity involved in the data breach they must alert the data owner so that the data owner can notify the affected individuals.

The IT Security Director shall provide this notice without undue delay as soon as verification of the unauthorized release is confirmed, except as delineated in #8 below.

4. In the case of a computer found to be infected with malware that exposes data to unauthorized access, individuals that may have had their information exposed due to use of the computer must be alerted in accordance with data breach rules.
5. Provide notification that consists of:
 - a. A general description of what occurred and when;
 - b. The type of personal information that was involved;
 - c. What actions have been taken to protect the individual's personal information from further unauthorized access;
 - d. A telephone number that the person may call for further information and assistance, if one exist; and
 - e. What actions DMV recommends that the individual take. The actions recommended should include monitoring their credit report and reviewing their account statements.
6. Provide this notification by one or more of the following methodologies, listed in order of preference:
 - a. Written notice to the last known postal address in the records of the individual or entity;

- b. Telephone Notice;
- c. Electronic notice; or
- d. Substitute Notice - if the individual or the entity required to provide notice demonstrates that the cost of providing notice will exceed \$50,000, the affected class of Virginia residents to be notified exceeds 100,000 residents, or the individual or the entity does not have sufficient contact information or legal consent to provide notice.

Substitute Notice consists of all of the following:

- i. Email notice if the individual or the entity has email addresses for the members of the affected class of residents;
 - ii. Conspicuous posting of the notice on the website of the individual or the entity if the individual or the entity maintains a website; and
 - iii. Notice to major statewide media.
7. In the event an individual or entity provides notice to more than 1,000 persons at one time pursuant to section E. of *Code of Virginia*, §18.2-186.6, the individual or entity shall notify, without unreasonable delay, the Office of the Attorney General and all consumer reporting agencies that compile and maintain files on consumers on a nationwide basis, as defined in 15U.S.C. §1681(a)(p), of the timing, distribution, and content of the notice.
 8. Not provide notification immediately following verification of unauthorized data disclosure only if law-enforcement is notified and the law-enforcement agency determines and advise 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.

3.9 IT Asset Management

3.9.1 Purpose

IT Asset Management delineates the steps necessary to protect IT systems and data by managing the IT assets themselves in a planned, organized, and secure fashion. This component of the DMV IT Security Policy defines requirements in the following three areas:

- IT Asset Control
- Software License Management
- Configuration Management and Change Control

3.9.2 IT Asset Control

3.9.2.1 Purpose

IT Asset Control requirements identify the steps necessary to control and collect information about IT assets.

3.9.2.2 Requirements

Commensurate with sensitivity and risk, the IT Security Director shall or shall require that its service provider (VITA) document inventory management practices that address the following components, at a minimum:

1. IT assets may be removed from DMV premises only with the explicit approval of the employee's supervisor and in accordance with DMV IT security practices.
2. Each supervisor shall maintain a written record of all IT assets assigned to each supervised employee, noting explicitly those IT assets permitted to be removed from DMV premises.
3. It is prohibited to connect any non-COV IT (i.e., personally-owned) asset to a COV IT asset. Examples of this include, but is not limited to, these items:
 - a. Connecting a personally-owned computer to the DMV network is prohibited.
 - b. Using a personally-owned USB drive with a DMV desktop computer or laptop is prohibited.
4. The only exceptions to the above requirement are those in accordance with the current version of *IT Standard use of Non-Commonwealth Computing Devices to Telework (SEC511-00)*.
5. It is prohibited to bring non-COV desktop computers or laptop computers onto DMV premises with the exception of those approved by the ISO for authorized IT staff for testing purposes.
6. Prior to the disposal of COV IT assets all data must be removed in accordance with the current version of the *Removal of Commonwealth Data from Surplus Computer Hard Drives and Electronic Media Standard (SEC514-03)*.
7. VITA shall prepare a list of all DMV IT assets – hardware and software – and provide it to the Agency Information Technology Resource (AITR) no less than annually.
8. The list will be reviewed by the AITR for completeness and accuracy.

3.9.3 Software License Management

3.9.3.1 Purpose

Software License Management requirements identify the steps necessary to protect against use of computer software in violation of applicable laws.

3.9.3.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document software license management practices that address the following components, at a minimum:

1. Only DMV approved software shall be installed on DMV IT assets.
2. Once an image is approved by DMV, VITA DSG will install the image as needed on DMV IT assets.
3. Exceptions/additions to the DMV image must be approved in writing by the ISO.
4. VITA shall assess, no less than annually, whether all software is used in accordance with license agreements.

3.9.4 Configuration Management and Change Control

3.9.4.1 Purpose

Configuration Management and Change Control requirements identify the steps necessary to document and monitor the configuration of IT systems, and to control changes to these items during their lifecycles.

3.9.4.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) document configuration management and change control practices so that changes to the IT environment do not compromise IT security controls.

At a minimum:

1. Baseline security standards shall be reviewed and revised at least annually and more frequently as needed.
2. Changes to baseline security standards are handled through the DMV/COV change management process and be authorized based on the technical impact of the change and associated risk.
3. Change Management (CM) is conducted through established CM procedures as required for a particular network, system, facility, etc.
4. All changes go through a change approval process.
5. All requests for change (RFC) are categorized according to their criticality.

6. With the exception of Emergency changes, all changes are first approved through the proper levels of management and documented before implementation of the change.
7. As part of the change management process, when any system undergoes a material change, the security configurations are reviewed and enhanced as necessary and all security configurations are verified.
8. As part of the change management process, all software that would be introduced onto a DMV IT system shall be approved by the ISO or designee.

3.10 Additional Security Requirements in Third-Party Contracts

3.10.1 Purpose

To provide additional explicit requirements for third parties requesting/having access to DMV data.

3.10.2 Requirements

The IT Security Director shall or shall require that its service provider (VITA) ensure that all third-party contracts involving access to DMV data meet the following requirements:

1. Before any third party is given access to DMV systems, a contract defining the terms and conditions of such access must have been signed by a responsible manager at the third party organization. These terms and conditions must also be approved by both the IT Security Director and the Data Owner as well as any other individuals designated by the Commissioner.
2. Prior to sending any sensitive data to a third party for copying, printing, formatting, or other handling, the third party must sign a DMV non-disclosure agreement.
3. Private or sensitive data in the custody of DMV must not be disclosed to third parties unless these third parties have signed an explicit chain of trust agreement approved by the IT Security Director.
4. As a condition of gaining access to DMV's computer network, every third party must secure its own connected systems in a manner consistent with DMV IT security requirements. DMV reserves the right to audit the security measures in effect on these connected systems without prior warning. DMV also reserves the right to immediately terminate network connections with all third party systems not meeting such requirements.
5. DMV's business partners, suppliers, customers, and other business associates must be made aware of their information security responsibilities via specific language appearing in contracts which define their relationship with DMV.

3.11 Collection of Evidence

3.11.1 Purpose

To provide additional explicit requirements for the collection of evidence for investigations, prosecution, and disciplinary actions.

3.11.2 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.

The relevant information must then be securely stored off-line until official custody is given to another authorized person.

The information to be immediately collected includes the current system configuration as well as backup copies of all potentially involved files.

2. For every production computer system, DMV ISO must identify the sources of digital evidence that reasonably could be expected to be used in a court case.

These sources of evidence must then be subject to a standardized capture, retention, and destruction process comparable to that use for vital records.

3. By making use of DMV systems, users consent to allow all information they store on DMV systems to be divulged to law enforcement.
4. 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 suspected party.
5. Every analysis or investigation using data storage media that contains information that might at some point become important evidence to a computer crime or computer abuse trial, must be performed with a copy rather than the original version.

This will help to prevent unexpected modification to the original information.

6. All DMV internal investigations of information security incidents, violations, and problems, must be conducted by trained staff authorized by the IT Security

Director or Law Enforcement Services (LES).

7. Any person who is related to or is friends of the suspects, for conflict of interest reasons, is barred from participating on an information security incident investigation team.

3.12 Additional Requirements for Protecting COV Data

3.12.1 Purpose

To provide additional explicit requirements for protecting COV data.

3.12.2 Requirements

The IT Security Director shall or shall require its service provider (VITA) ensure that the following requirements are met for protecting COV data:

1. Outside of regular working hours, unless they are working at the time, all DMV and service provider (VITA) employees, including contractors, and all other personnel, shall clean their desks and working areas such that all sensitive or valuable data is properly secured.
2. Unless information is in active use by authorized personnel, desks shall be absolutely clear and clean during non-working hours with all information locked away.
3. When not in use, sensitive data left in an unattended room shall be locked away in appropriate containers.
4. When not being used by authorized employees, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive data and all computer media containing sensitive data shall be locked in file cabinets, desk, safes, or other heavy furniture.
5. All employees who handle sensitive data shall adequately conceal this information from unauthorized disclosure to nearby non-authorized parties.
6. All employees shall refrain from discussing sensitive data in public places such as in building lobbies or on public transportation.
7. DMV employees shall not discuss sensitive data in administrative areas including, but not limited to, corridors, cafeterias, visitor reception areas, and restrooms, because these areas are likely to include persons who have not been expressly

authorized to receive this information.

8. If sensitive data is discussed verbally in a meeting, seminar, lecture, or related presentation, the speaker shall clearly communicate the sensitivity of the information and remind the audience to use discretion when disclosing it to others.
9. 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.
10. If the computer system to which they are connected or which they are using contains sensitive data, users shall not leave their individual computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.
11. If personal computers are connected to a DMV network, when unattended they shall always be logged off.

3.13 Additional Requirements for Protecting COV Data when Using Telephones

3.13.1 Purpose

To provide additional explicit requirements for protecting COV data when using telephones.

3.13.2 Requirements

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.

4.0 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 (Groupwise). 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 Network Support @ 804-367-6857 for assistance.

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.

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.

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.

5.0 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.

Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media
Page 1 of 2 Pages

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

IT Security Director/ISO Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	<input type="checkbox"/> YES - Request is Approved <input type="checkbox"/> NO - Request is Not Approved

Assistant Commissioner/CIO Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	<input type="checkbox"/> YES - Request is Approved <input type="checkbox"/> NO - Request is Not Approved

Commissioner Review/Approval	
Printed Name:	
Signature:	
Date:	
Approved?	<input type="checkbox"/> YES - Request is Approved <input type="checkbox"/> NO - Request is Not Approved

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

Authorization to Store Sensitive Data on a Mobile Data Storage Device or Media Page 2 of 2 Pages
