Virginia Department of Motor Vehicles (DMV)

Information Security & Risk Management Policy

Information Security and Risk Management Office (ISRM)

ISRM Publication Version Control

DMV ISRM reviews agency polices at least annually, and the date and summary of any revisions made are reflected in the table below.

Version Number	Date	Revision Summary
1.X	2016 base polices with individual updates based on changes in requirements	Existing policies that were included in the revision process: DMV IT Acceptable Use Policy DMV IT Access Control Policy DMV IT Audit and Accountability Policy DMV IT Business Impact Analysis Policy DMV IT Configuration Management Policy DMV IT Contingency Planning Policy DMV IT Identification and Authentication Policy DMV IT Media Protection Policy DMV IT Mobile Device Access Controls Policy DMV IT Personnel Security Policy DMV IT Physical and Environmental Security Policy DMV IT Risk Assessment Policy DMV IT System Assessment and Authorization Policy DMV IT Security Awareness and Training Policy DMV IT Security Exception Policy DMV IT System and Communications Protection Policy DMV IT System and Communications Encryption Policy DMV IT System and Data Classification Policy DMV IT System and Information Integrity Policy DMV IT System Maintenance Policy DMV IT Security Planning Policy DMV IT Wireless and Remote Access Control Policy DMV Physical and Environmental Protection Policy DMV System and Information Integrity Policy DMV System and Services Acquisition Policy
2	02/27/2022	New policy/standard framework implemented to reduce the number of polices and target specific audiences
2.1	3/01/2024	Updated for new SEC530 security standard

1 Introduction

The Virginia Department of Motor Vehicles (DMV) is responsible for implementing the Commonwealth Information Security Policy and Standards as well as other regulatory and data security policies and standards for internally developed systems, third-party developed and/or operated systems, systems which DMV accesses but are not under DMV control, and for sharing DMV data and information outside of DMV. The Commonwealth of Virginia Security Standards sourced most of their controls from the most current National Institute of Standards and Technology Special Publication 800-53 (Security and Privacy Controls for Federal

Information Systems and Organizations). All controls from these standards are mandatory unless determined otherwise by DMV Information Security and Risk Management (ISRM) staff. These controls combined with the other applicable regulatory requirements are considered DMV's minimum security and privacy baseline.

2 Statement of Policy

It is the policy of the COV (§2.2-603.F) that each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of §2.2-2009. In addition, the Director of every department is responsible for the security of the agency's electronic information, and for establishing and maintaining an agency information security program compliant with this policy and meets all the requirements established by COV ITRM Security Standards.

This policy and related standards provide the security framework that DMV will use to establish and maintain their information security program.

3 Acronyms

The following table contains acronyms and their descriptions used throughout DMV Information Security Policies

- CISO: Chief Information Security and Risk Officer
- COV: Commonwealth of Virginia
- ISRM: Information Security & Risk Management Office
- DHRM: Virginia Department of Human Resources Management
- ISO: Information Security Officer
- IT: Information Technology
- ITRM: Information Technology Resource Management
- LAN: Local Area Network
- PC: Personal Computer
- ROB: Rules of Behavior
- SEC530: Current version of ITRM Information Security Standard 530
- TPRM: DMV Third-Party Risk Management Program
- VITA: Virginia Information Technologies Agency
- VPN: Virtual Private Network

4 Definitions

See COV glossary located at: https://www.vita.virginia.gov/policy--governance/glossary/cov-itrm-glossary/

5 Roles and Responsibilities

Roles and responsibilities for Information Security controls are assigned to individual employees and contractors of the DMV, service providers, and external data users. The individuals assigned to roles will vary depending on several factors including the system / service provider (internal or external) and the organization with which DMV holds data sharing agreement.

A. The DMV Chief Information Security Officer (CISO) will review, update and revise policies, standards, processes and procedures on an annual basis or more frequently if required by changes in local, state or federal law.
B. DMV TPRM will establish a periodic reporting requirement to measure compliance to and effectiveness of this policy.
C. DMV Management is responsible for implementing the requirements of this policy, or documenting non-compliance via ISRM exception process.
D. DMV Management is responsible for the periodic auditing and reporting of compliance with this policy.
E. DMV Executives are responsible for defining the format and frequency of the reporting requirements and communicating those requirements, in writing, to DMV Management.
F. DMV Managers and supervisors in cooperation with ISRM, are required to train employees on policy and document issues with Policy compliance.
G. All DMV employees are required to read and acknowledge the reading of this policy.
H. System owners are accountable for ensuring that their systems are securely configured and maintained in compliance with all related security policies.

6 Information Security Program

The policy of DMV is to secure its electronic information using methods based on the sensitivity of the information and the risks to which the information are subject, including the dependence of critical agency business processes on the information and related systems.

The DMV Information Security Program framework addresses the requirements set forth in § 2.2-603.F that each Agency Head is responsible for securing the electronic data that is held by the agency and shall comply with the requirements of § 2.2-2009. In addition, the Director of every department is responsible for the security of the agency's electronic information, and for establishing and maintaining an agency information security program compliant with this policy and meets all of the requirements established by COV ITRM Security Standards.

The DMV Information Security Program includes:

- Development of policies, standards, and guidelines that provide for the security of agency electronic information;
- Addressing the scope and frequency of security audits;
- Preventing unauthorized use, intrusions, or other security threats;
- Provide for the protection of confidential data;

- Developing and maintaining a risk management program designed to identify information technology security gaps and develop plans to mitigate the gaps;
- Requiring that any contract for information technology entered into by the agency address compliance with applicable Commonwealth and federal laws, as well as regulations pertaining to information security and privacy**;**
- Reporting on the status of information security and risk management governance;
- Promptly receive reports of incidents that threaten agency data and take such actions as are necessary, convenient, and desirable to ensure the security of the Commonwealth's electronic information (§ 2.2-603);
- Providing all agency staff members, contractors, and vendors information, guidance, and assistance related to information security policies, standards, and guidelines;
- Identification and notification of all hardware and software that has been prohibited pursuant to Chapter 55.3 (§ 2.2-5514); and
- Developing a curriculum and materials for training all agency employees and contractors in information security awareness.

7 Policies and Standards

DMV Information Security & Risk Management policies, and standards are included below.

- DMV Security & Risk Management Policy (this document)
- DMV Acceptable use Policy
- DMV Security Technical Control Standard
- DMV System and Services Security Lifecycle Standard
- DMV Security and Risk Management Standard

8 User Agreement to Monitoring

Users must comply with all requirements of *DHRM 1.75 Use of Electronic Communications and Social Media*, which defines the appropriate use of COV information technology by COV employees, and any applicable agency policies. Any use of COV information technology resources constitutes consent to monitoring of that use and any activities that may be conducted through COV IT resources, whether or not a warning banner is displayed. There is no expectation of privacy when utilizing COV information technology resources.

DMV reserves the right to:

- Review the data contained in or traversing DMV information resources including social media.
- Review the activities on DMV information IT resources.
- Act on information discovered as a result of monitoring and disclose such information to law enforcement and other organizations as deemed appropriate by the CISO.
- Monitor at any time, without notice and without the user's permission.