

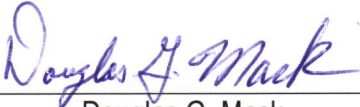
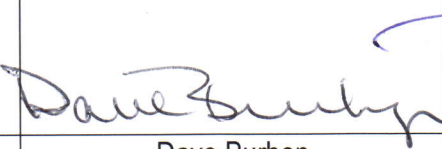



Virginia Department of Motor Vehicles

Acceptable Use Policy

Version 3.0 – May 2015

Approval of Acceptable Use Policy Version 3.0

		
Douglas G. Mack IT Security Director ISO	Dave Burhop Deputy Commissioner CIO	Richard D. Holcomb Commissioner Agency Head
04/27/2015	4-27-15	4-27-15
Date	Date	Date

1) Introduction

As an agency of the Commonwealth of Virginia (“The Commonwealth”, “COV”), the Virginia Department of Motor Vehicles (“DMV” or “The Agency”) is required by statute, regulation, and policy to implement a comprehensive Information Security (IS) Policy (“IS Policy” or “Policy”). The Agency's Information Security Policy intends to protect the confidentiality, integrity, and availability of information captured, stored, processed, transmitted or otherwise handled by DMV personnel, Agency systems or third-parties working on DMV's behalf.

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of COV Information Technology (IT) systems to protect COV and DMV assets and information.

2) Authority

DMV's *IT Security Policy* is the source for this *Acceptable Use Policy and User Agreement Acknowledgement* and also provides the context for it.

Additional information on the acceptable and permitted use of COV IT systems, as well as other IT security requirements, is found in DMV's *IT Security Policy*.

3) Scope

These policies apply to all personnel and locations of the Virginia Department of Motor Vehicles, including employees, contractors, consultants, vendors and any other personnel with access to DMV information, IT systems or networks.

4) Compliance & Enforcement

Classified employees may be subject to disciplinary action up to and including discharge, under the Commonwealth's Standards of Conduct (DHRM 1.60); wage employees, contractors and consultants assigned to or working for the Agency may be subject to administrative and contractual sanctions. Criminal or civil action may be initiated in appropriate instances.

Selective enforcement or non-enforcement of any policy provisions shall not permit non-compliance by any parties covered by the scope of these policies.

All suspected or known violations of the law shall be immediately reported to DMV Assistant Commissioner, Enforcement and Compliance.

5) 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 by DMV is also governed by the Federal Driver's Privacy Protection Act (18 USC §§ 2721 - 2725) and by Va. Code §§ 46.2-208 through 213. These statutes prohibit DMV from disclosing personal, driver, and vehicle information collected by it in the administration of the motor vehicle laws of Virginia, unless the release of such information meets one of the conditions specified in Va. Code §§ 46.2-208 through 213 and applicable fees are paid.

6) General Requirements

- a. All DMV IT users shall abide by the Department of Human Resource Management (DHRM) Policy 1.75, "Use of Internet and Electronic Communication Systems."
- b. 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.
- c. DMV User IDs and Passwords are unique and assigned only to the individual approved for the specific access.
- d. DMV Users shall not share their User IDs or Passwords with another person under any circumstances.
- e. All DMV IT users shall create and use complex passwords.

- f. Limited – incidental or occasional – personal use of DMV IT resources – i.e. non work related – is permitted if:
 - i. It does not adversely affect the performance of official business and duties;
 - ii. 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.
- g. DMV blocks specific categories of web sites and certain specific web sites for one or more of three reasons:
 - i. Legal Risk – To ensure compliance with applicable Federal/State laws, policies, standards, and guidelines;
 - ii. Security Risk – To protect Commonwealth IT assets from malware;
 - iii. Bandwidth Risk – To ensure adequate bandwidth for agency required processes.
- h. Very often more than one of the reasons is involved with the determination to block a category or web site.
- i. DMV may, at any time, without notice, update the list of prohibited web sites.
- j. Games, other than DMV approved ones (such as those used for training), may not be stored or used on any DMV computer or computer system.
- k. The following statements, although not inclusive, define specific unacceptable uses of COV IT resources:
 - i. Accessing, downloading, printing, or storing sexually explicit material in violation of the Code of Virginia, §2.2-2827.
 - ii. Gambling.
 - iii. Use for private or personal gain.
 - iv. Use for initiating and completing a personal (non-work related) transaction with a vendor.

- v. Use for illegal purpose or any communication that violates applicable laws and regulations.
- vi. Use for product advertisement.
- vii. To transmit threatening, obscene or harassing materials.
- viii. Unauthorized attempts to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.
- ix. Tampering with or otherwise attempting to circumvent security controls.
- x. Installing or using proprietary encryption hardware/software.
- xi. 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.

- xii. Knowingly uploading or downloading commercial software in violation of its copyright and/or licensing agreement.
- xiii. Adding hardware to, removing hardware from, or modifying hardware on a COV system.
- xiv. Connecting any non-COV-owned device 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).

The following are some examples of non-COV-owned devices that may not be connected to a COV IT system or network. Please

Note: The list is not an all-inclusive one.

1. Personally-owned computers (desktop/laptop).
2. Personally-owned printers.
3. Personally-owned scanners.
4. Personally-owned flash drives.

5. Personally-owned iPhone, BlackBerry, or other similar communication device.
 6. Personally-owned media device.
 7. Personally-owned monitors.
 8. Personally-owned speakers.
 9. Personally-owned keyboard/mouse.
- xv. Forwarding chain letters.
 - xvi. Using Email Groups/Lists, especially "ALL-DMV," without appropriate authorization.
 - xvii. Sending large numbers of messages to an individual or a group – i.e. Mail Bombing.
 - xviii. Attempting to subscribe anyone else to mailing lists.
 - xix. Downloading or installing without the authorization of IT Security Director:
 1. Copyrighted materials.
 2. Games.
 3. Screen Savers.
 4. Peer-to-Peer file-sharing programs.
 5. Non-DMV supported software.
 - xx. Playing online electronic games.
 - xxi. Using unauthorized instant messaging – including, but not limited to, AOL Instant Messenger, Yahoo Instant Messenger, ICQ, Microsoft, etc.

xxii. Using peer-to-peer file sharing applications such as, but not limited to:

Ares Galaxy Network Manolito Network

Ares Galaxy Piolet

Gnutella Blubster

Adagio Rocketnet

BearShare

FileScope BitComet

FilesWire Bitflu

giFT BitSpirit

Gnucleus BitTorrent 5/Mainline

GTK-gnutella BitTorrent 6

LimeWire Deluge

Mactella Gnome BitTorrent

Morpheus Halite

Phex KTorrent

Shareaza MP3 Rocket

Sharelin OneSwarm

XFactor QTorrent

Bit Torrent--Distributed File Sharing System

eDonkey Network (e) qBittorrent

eDonkey2000 rTorrent

eMule Tixati

eMule Plus Transmission

iMule Tribler

JMule µTorrent

IMule Vuze (formerly Azureus)

xMule

Hydranode

Jubster

Lphant

MLDonkey

Pruna

Direct Connect

DC++

MLDonkey

NeoModus Direct connect

ShakesPeer

Linux DC++

jucy

Valknut

DCTC

DC#

LDCC

ApexDC++

- xxiii. Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
 - xxiv. Posting COV information to external newsgroups, bulletin boards or other public forums without authorization from the IT Security Director.
- l. It is prohibited to access DMV/COV email on a personally owned smart phone using the Microsoft software Active Sync or any other program to keep Outlook Web Access open.
 - m. If software to sync a personally owned smart phone with Outlook is needed, the established process for obtaining the software must be followed.

If there are any questions on this, please contact the IT Security Office.

- n. 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.
- o. COV, in the IT Security Standard (SEC501), explicitly prohibits users from having Local Administrator Rights or AA Accounts without an approved exception on file.

If a user believes he or she has a business need to have such elevated rights, please contact the IT Security Office for the process for documenting the request.

7) Specific Requirements for DMV Systems and Records

Employees are responsible for adhering to the following, as well as specific policy components that relate to their job duties:

- a) Protect confidential and personal information to which you have access by following all security procedures, including but not limited to:
 - i) Unless information is in active use by authorized personnel, desks shall be absolutely clear and clean during non-working hours with all confidential

- information locked away.
- ii) When not in use, sensitive data left in an unattended room shall be locked away in appropriate containers.
 - iii) 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.
 - iv) All employees who handle sensitive data shall adequately conceal this information from unauthorized disclosure to nearby non-authorized parties.
 - v) All employees shall refrain from discussing sensitive data in public places such as in building lobbies or on public transportation.
 - vi) 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.
 - vii) 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.
 - viii) 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.
 - ix) 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.
- b) Do not create, access, alter, delete or release any records that DMV maintains except as necessary to perform your assigned duties.
 - c) Do not disclose customer information to any individual or entity, except when federal or state statutes or DMV operating procedures specifically allow it.
 - d) Request sufficient identification to assure yourself of the person's identity before releasing any customer information and before conducting transactions. Be sure to follow DMV policies, procedures, and guidelines in the Dissemination of Information tables on the Intranet when determining what is "sufficient identification."

-
- e) Give confidential and personal records to other DMV users only if those users have an official need to know in connection with their duties.
 - f) Immediately report any knowledge of a violation of information security to your supervisor or higher management.
 - g) Safeguard information obtained through the NCIC (National Criminal Information Center), NLETS (National Law Enforcement Tracking System), NDR (National Driver Register), CDLIS (Commercial Driver License Information System), or other sources of disclosure from unauthorized parties in the same way that you safeguard information originating in Virginia.
 - h) Users must, like any other customers, complete an application and pay fees for personal transcripts or any other services of the department.
 - i) Personal records in DMV computer systems are to be accessed by users only for the purpose of assisting customers as prescribed by Commonwealth laws and DMV policies and procedures; and shall not to be accessed:
 - i) For personal use, or
 - ii) For personal gain, or
 - iii) To avoid paying fees, or
 - iv) To help friends, relatives, or others learn about themselves or other individuals.
 - j) DMV's customer records are considered privileged and the access, use, and release of these records is restricted by Federal and State laws. The access and use of these records is considered as consent to agency monitoring at all times. Violation of the laws governing these records could result in civil penalties and/or criminal prosecution. DMV employees violating these laws or the agency's Information Technology Policy also may be subject to disciplinary action. Information on any possible violations may be provided to law enforcement officials.
 - k) Examples of provisions for civil and/or criminal penalties for violation of the laws governing records include, but are not limited to:
 - i) Obtaining information under false pretenses, or unauthorized disclosure of information is punishable by a fine, imprisonment, or both. (See: Code of Virginia, §18.2-152.5.)

- ii) Persons who are harmed may also bring civil suit for damages sustained, and the court may also award punitive damages, costs, and attorney's fees. (See: Code of Virginia, §18.2-152.4. & §18.2-152.12)
- iii) Altering, erasing, or making copies of data is in some cases chargeable as a Class 6 felony. (See: Code of Virginia, §18.2-152.14. & §18.2-168.)
- iv) Unauthorized access or disclosure of another person's employment, salary, credit, or other personal or financial information is chargeable as a misdemeanor. (See: Code of Virginia, §18.2-152.5.)