

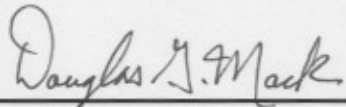
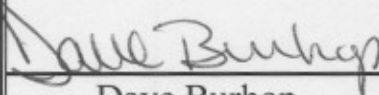
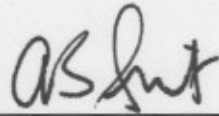
VIRGINIA DEPARTMENT OF MOTOR VEHICLES

**ACCEPTABLE USE POLICY
AND USER AGREEMENT ACKNOWLEDGEMENT**

**02/26/09 Version
Approved March 11, 2009**



**Approval of Acceptable Use Policy and User Agreement
Acknowledgement (02/26/2009 Version)**

		
Douglas G. Mack IT Security Director ISO	Dave Burhop Assistant Commissioner CIO	D.B. Smit Commissioner Agency Head
2-26-09	3-4-09	3-11-09
Date	Date	Date

SECURITY is not complete without U!



Acceptable Use Policy and User Agreement Acknowledgement

02/26/09 Version – Approved 03/11/09

1) Purpose

Acceptable Use requirements identify the steps necessary to define acceptable and permitted use of Commonwealth of Virginia (COV) Information Technology (IT) systems to protect DMV and COV 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) Definitions

a) Business Use

COV-provided computer systems that allow access to the Internet and electronic communication systems are the property of the Commonwealth and are provided to facilitate the effective and efficient conduct of State business. Users are permitted access to the Internet and electronic communication systems to assist in the performance of their jobs.

b) Personal Use

Personal Use Personal use means use of COV-provided computer systems that is not job-related.

4) Scope

All person or entities authorized to transact business, access, use, provide, or receive information contained in any DMV information system, record set, or electronic communication system are subject to this policy.

This includes, but is not limited to:

a) Employees (full-time, part-time, wage employees),

- b) Contracted personnel (contractors, consultants, vendors, or temps),
- c) Non-employees (volunteers or interns).

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.

6) Violation of Law

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

7) Requirements

a) General Requirements

- i) All DMV IT users shall abide by the Department of Human Resource Management (DHRM) Policy 1.75, "Use of Internet and Electronic Communication Systems."
- ii) 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.
- iii) DMV User IDs and Passwords are unique and assigned only to the individual approved for the specific access.
- iv) DMV Users shall not share their User IDs or Passwords with another person under any circumstances.
- v) All DMV IT users shall create and use complex passwords:
 - (1) The password shall be at least nine characters in length, and
 - (2) Shall not be based on a single dictionary word (ex. Bad Password: P4\$sw0rD vs. Good Password: t0YtR4p!), and
 - (3) Shall utilize at least three of the following four:
 - (a) Lowercase alpha (e.g. abc)

- (b) Uppercase alpha (e.g. ABC)
- (c) Numeric (e.g. 123)
- (d) Special/Non-Alphanumeric characters (e.g. ! \$ # %)

vi) Limited – incidental or occasional – personal use of DMV IT resources – i.e. non work related – is permitted if:

- (1) It does not adversely affect the performance of official business and duties;
- (2) 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.

vii) DMV blocks specific categories of web sites and certain specific web sites for one or more of three reasons:

- (1) Legal Risk – To ensure compliance with applicable Federal/State laws, policies, standards, and guidelines;
- (2) Security Risk – To protect Commonwealth IT assets from malware;
- (3) 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.

viii) Games may not be stored or used on any DMV computer or computer system.

ix) The following statements, although not inclusive, define specific **unacceptable** uses of COV IT resources:

- (1) Accessing, downloading, printing, or storing sexually explicit material in violation of the Code of Virginia, §2.2-2827.
- (2) Gambling.
- (3) Use for private or personal gain.

- (4) Use for illegal purpose or any communication that violates applicable laws and regulations.
- (5) Use for product advertisement.
- (6) To transmit threatening, obscene or harassing materials.
- (7) Unauthorized attempts to seek information on, obtain copies of, or modify files, other data or passwords belonging to other users.
- (8) Tampering with or otherwise attempting to circumvent security controls.
- (9) Installing or using proprietary encryption hardware/software.
- (10) 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.

- (11) Knowingly uploading or downloading commercial software in violation of its copyright and/or licensing agreement.
- (12) Adding hardware to, removing hardware from, or modifying hardware on a COV system.
- (13) 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).
- (14) Forwarding chain letters.
- (15) Using Email Groups/Lists, especially “ALL-DMV,” without appropriate authorization.
- (16) Sending large numbers of messages to an individual or a group – i.e. Mail Bombing.
- (17) Attempting to subscribe anyone else to mailing lists.

- (18)** Downloading or installing without the authorization of IT Security Director:
- (a) Copyrighted materials.
 - (b) Games.
 - (c) Screen Savers.
 - (d) Peer-to-Peer file-sharing programs.
 - (e) Non-DMV supported software.
- (19)** Playing online electronic games.
- (20)** Using unauthorized instant messaging – including, but not limited to, AOL Instant Messenger, Yahoo Instant Messenger, ICQ, Microsoft, etc.
- (21)** 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.
- (22)** Engaging in any outside fundraising activity, endorsing any product or service, participating in any lobbying activity, or engaging in any prohibited partisan political activity.
- (23)** Posting COV information to external newsgroups, bulletin boards or other public forums without authorization from the IT Security Director.
- x)** 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.
- xi)** 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.

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.

(1) 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.

(2) 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.

- xii) 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.
- xiii) Transmission of unencrypted sensitive data over the Internet is prohibited.
- xiv) 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.

b) 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:

- i) Protect confidential and personal information to which you have access by following all security procedures, including but not limited to:
 - (1) 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.
 - (2) When not in use, sensitive data left in an unattended room shall be locked away in appropriate containers.
 - (3) 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.
 - (4) All employees who handle sensitive data shall adequately conceal this information from unauthorized disclosure to nearby non-authorized parties.
 - (5) All employees shall refrain from discussing sensitive data in public places such as in building lobbies or on public transportation.
 - (6) 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.

- (7) 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.
- (8) 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.
- (9) 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.
- ii) Do not create, access, alter, delete or release any records that DMV maintains except as necessary to perform your assigned duties.
- iii) Do not disclose customer information to any individual or entity, except when federal or state statutes or DMV operating procedures specifically allow it.
- iv) 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."
- v) Give confidential and personal records to other DMV users only if those users have an official need to know in connection with their duties.
- vi) Immediately report any knowledge of a violation of information security to your supervisor or higher management.
- vii) 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.
- viii) Users must, like any other customers, complete an application and pay fees for personal transcripts or any other services of the department.
- ix) 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:

- (1) For personal use, or
 - (2) For personal gain, or
 - (3) To avoid paying fees, or
 - (4) To help friends, relatives, or others learn about themselves or other individuals.
- x) 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.
- xi) Examples of provisions for civil and/or criminal penalties for violation of the laws governing records include, but are not limited to:
- (1) 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.)
 - (2) 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)
 - (3) 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.)
 - (4) 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.)



**Acceptable Use Policy
User Agreement Acknowledgement**

02/26/09 Version – Approved 03/11/09

- 1) I acknowledge that I have been given a copy of the DMV Acceptable Use Policy and I understand that it is my responsibility to read and abide by this policy.
- 2) If I have any questions about the DMV Acceptable Use Policy, I understand that I need to ask my Supervisor or the DMV Information Technology (IT) Security Director for clarification.
- 3) By signing this agreement (either electronically or physically) I hereby certify that I understand the preceding terms and provisions and that I accept the responsibility of adhering to the same.
- 4) I further acknowledge that any infractions of this agreement may result in the penalties described in number 5 “Enforcement” of the Acceptable Use Policy.

Employee Name (Printed)

Employee Signature

Date

Acknowledgement and Acceptance on the DMV Knowledge Center (DMVKC) replaces the printed *User Agreement Acknowledgment* form.

The printed *User Agreement Acknowledgment* form and hard copy of the *Acceptable Use Policy* is to be used for individuals not having access to the DMVKC.

The signed printed *User Agreement Acknowledgment* form is to be sent to (either by mail or fax):

**IT Security Director
DMV Headquarters (804)-367-2410**