STATE OF COLORADO

DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
6848 South Revere Parkway
Centennial, Colorado 80112
Phone (720) 847-8801
Fax (720) 847-8811

Bill Ritter
Governor

Major General
Micheal H. Edwards
The Adjutant General

Policy Letter: DMVA 25-1

Effective Date: 1 March 2008

Summary: Provides policy on use of state information technology equipment and software.

Applicability: All State employees of DMVA

Staff Proponent: Chief Information Officer

Supersedes: DMVA 25-1, dated 1 March 2005.

Official:

Walter Paul
Acting Deputy Director

Distribution: All State Employees of DMVA

Department of Military & Veterans Affairs
Information Technology Acceptable Use Policy

1.0 Overview
Department of Military & Veterans Affairs (DMVA) is committed to protecting the State's employees, partners and the department from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of the State of Colorado. These systems are to be used for business purposes in serving the interests of the department, and of our clients and customers in the course of normal operations. Effective security is a team effort involving the participation and support of every DMVA employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose
The purpose of this policy is to outline the acceptable use of computer and information technology equipment at DMVA. These rules are in place to protect the employee and State of Colorado. Inappropriate use exposes the State to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope
This policy applies to Department employees, contractors, consultants, temporaries, and other workers such as the Colorado National Guard at DMVA including all personnel affiliated with third parties who may use Department resources. This policy applies to all equipment that is owned or leased by DMVA. It also applies to equipment not owned by DMVA that is attached to any DMVA information technology systems such as network resources either wired or wireless.

4.0 Definitions
Term Definition
Spam Unauthorized and/or unsolicited electronic mass mailings.
Personally Identifiable Information (PII) Items which might be considered PII include, but are not limited to, a person's:

- Social Security Number
- Date of Birth
- Physical address
- Telephone number
- Vehicle registration plate number
- Driver's license number
- Fingerprints

- Credit card numbers

Portable Storage Device can be but is not limited to;

- Portable USB Storage, i.e. thumbnail drive, SD cards
- PDA, Personal Digital Assistant
- Compact Disk
- Digital Video Disk
- MP3 Player/IPOD
- Telephone
- Cameras
- Any devices that can store data that is reasonably mobile

5.0 Policy

5.1 General Use and Ownership

Users should be aware that the data they create on the state systems remains the property of DMVA and the State of Colorado. Because of the need to protect DMVA's network and data, the department does not guarantee the confidentiality of information stored on any network device belonging to DMVA.

5.2 Security and Proprietary Information

1. For security and network maintenance purposes, authorized individuals within DMVA may monitor equipment, systems and any traffic at any time and keep a record of that monitoring.
2. DMVA reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.
3. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by state confidentiality guidelines, details of which can be found in Human Resources policies.
4. You must not provide access to personally identifiable information outside of work activities. Personally identifying information (PII) is any piece of information which can potentially be used to uniquely identify, contact, or locate a single person.

   Examples of confidential or Personally Identifiable Information (PII) include but are not limited to: state private, personal sensitive, specifications, employee lists with personal data, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.
5. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed every six months; user level passwords should be changed every six months. Strong passwords are required. An example of a strong password a minimum 8 characters containing a numeric and non-numeric character.
6. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Windows users) when the host will be unattended.
7. Because information contained on portable computers, cell phones, PDA's, and thumb drives is especially vulnerable, special care must be exercised against their physical loss.

8. All data identified as confidential must be encrypted if saved on any portable storage device.
   If you do not know how to encrypt the data, ask for help from DMVA's IT POCs.
9. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

5.3. Unacceptable Use

The following activities are, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities. Under no circumstances is an employee of DMVA authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing DMVA-owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

Information Systems Activities

The following activities are strictly prohibited, with no exceptions:

1. The use of profanity, obscenity or other language that may be offensive to another user.
2. Any form of vandalism, including but not limited to, damaging computers, computer systems, or networks, and/or disrupting the operation of the network.
3. Copying and/or downloading commercial software or other material (e.g. music) in violation of federal copyright laws.
4. Use of the network for financial gain, commercial activity, or illegal activity.
5. Use of the network for political activity.
6. Use of the network to access pornographic or obscene material.
7. Creating and/or placing a computer virus on the network.
8. Accessing another person's individual account or accessing a restricted account without the prior consent of the responsible owner.
9. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by DMVA.
10. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which DMVA or the end user does not have an active license is strictly prohibited.
11. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.
12. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).
13. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

14. Using a DMVA computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user's local jurisdiction.
15. Making fraudulent offers of products, items, or services originating from any DMVA account.
16. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.
17. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
18. Port scanning or security scanning is expressly prohibited unless prior approval by a DMVA administrator is made.
19. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
20. Circumventing user authentication or security of any host, network or account.
21. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).
22. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
23. Providing information about, or lists of, DMVA employees to parties outside DMVA.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).
2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
3. Unauthorized use, or forging, of email header information.
4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.
5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
6. Use of unsolicited email originating from within DMVA's networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by DMVA or connected via DMVA's network.
7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

6.0 Enforcement

Any employee found to have violated this policy may be subject to corrective or disciplinary action, up to and including termination of employment.

Monitoring results will be reviewed monthly at the DMVA staff briefing to ensure compliance.

7.0 In processing
This Acceptable Use Policy must be signed and validated by the Human Resources Manger. This signature will be kept on file with the persons record. This record does not have an expiration date.

System access will not be provided until this document is appropriately signed.

_____	_____	_____
Human Resources Manager	Employee	Date

8.0 Out processing
All persons having access to information technology equipment and information must out process though the DMVA's accounting office to make sure that all equipment has been accounted for and you are released from accountability. This is validated by the Human Resources Manager and filed in their record.

_____	_____
Accounting Office Property Manager	Date

_____	_____
Human Resources Manager	Date