New Jersey Department of Military and Veterans Affairs (DMAVA)

Computer Resources Acceptable Use Policy
(Revised 1 October, 2012)

Purpose
To outline guidelines for the acceptable utilization of DMAVA computing systems and facilities located at or operated by DMAVA. The purpose of these guidelines is to ensure that all DMAVA users (support personnel and management) use the DMAVA computing facilities in an effective, efficient, ethical, and lawful manner.

Scope
This policy applies to all DMAVA employees and system users whether authorized or unauthorized who access and use DMAVA computing systems and facilities, to include the Internet, and encompasses all decisions and activities affecting or affected by access or use of the network by DMAVA employees and system users whether authorized or unauthorized. This policy is established under authority of State of New jersey P.L.2007.c.56 and is published IAW with guidance form State of New Jersey (IT) Circular 09-07-NJOIT, dated 24 August 2012. The policies set forth in this document are limited and qualified by the Federal Wire Tap Act, 18 U.S.C. §2710 et seq, and the New Jersey Wiretap Act, N.J.S.A 2A:156A-1 et seq.

By accessing the State's network or Internet system a user agrees to adhere to the State's policies, including agency specific policies, regarding their use.

Definitions
As used in this policy, unless the context clearly requires a different meaning, the following words shall have the meaning indicated:

"Access" means the ability to receive, use, and manipulate data and operate controls included in information technology.

A **"cache"** is a hiding and/or safe place to store valuables for concealment; a fast storage buffer in the central processing unit of a computer to store something more or less temporarily. Web pages, which employee's request, are stored in the browser's cache directory.

"Computing systems and facilities" are defined as any computer, server, or network provided by or supported by the DMAVA Customer Support Center.

A **"cookie"** is a special text file that a web site puts on the user's hard disk so that it can remember something about the user at a later time. Typically, a cookie records the user's preferences when using a particular site.

"Information infrastructure" means telecommunications, cable, and computer networks and the Internet, including the World Wide Web, e-mail, File Transfer Protocol, Usenet, bulletin board systems, on-line systems, and telephone networks.

"Instant messaging" is a type of communications service that enables a user to create a private chat room with another individual. Typically, the instant messaging system alerts a user whenever somebody on the user's private list is online. A user can then initiate a chat session with that particular individual. This type of communication constantly searches the Internet looking for persons on the private list. Instant messaging requires larger amounts of network resources (bandwidth).

"Information technology" means all electronic information processing hardware and software, including telecommunications.

The **"Internet"** is a worldwide system of interconnected computer networks in which users at any one computer can obtain and exchange information with any other computer.

"Malicious software" is software designed to infiltrate or damage a computer system without the owner' informed consent. The expression is a general term used by computer professionals to mean a variety of forms of hostile, intrusive, or annoying software or program code.

"Network" in information technology, is a system that transmits any combination of voice, video, and/or data between users. The network includes the network operating system in the client and server machines, the cables connecting them and all the supporting hardware in between, such s bridges, routers, and switches. In wireless systems, the antennas and towers are also part of the network. In this document, the network is the Garden State Network, which is ultimately managed by the NJ Office of Information Technology. DMAVA-IASD manages our portion of this network.

"Path Records" are the combination of history, cache, cookie, and e-mail header files that record the Internet pages visited.

"Personal Information" is information about a person that identifies or describes an individual, including, but not limited to, his or her name, social security number, physical description, home address, home telephone number, education, financial matters, and medical or employment history, readily identifiable to a specific individual.

"Sexually explicit content" means content having as a dominant theme (i) any lascivious description of or (ii) any lascivious picture, photograph, drawing, motion picture film, digital image or similar visual representation depicting a lewd exhibition of nudity, sexual excitement, or sexual conduct.

"State-provided" means access to the Internet via computer system networks owned, leased, or operated by the State of New Jersey and/or DMAVA. Use of these services shall be subject to monitoring for security or network management reasons.

"Streaming media" is streaming video with sound. With media streaming, a web user does not have to wait to download a large file before seeing the video or hearing the sound. Instead, the media is sent in a continuous stream and is played as it arrives. Streaming media requires larger amounts of network resources (bandwidth).

"Streaming video" is a sequence of "moving images" that are sent in compressed form over the Internet and displayed by the viewer as they arrive. An example of a streaming video is a stock market ticker. With streaming video, a web user does not have to wait to download a large file before seeing the video. Instead, the video is sent in a continuous stream and is played as it arrives. Streaming video requires larger amounts of network resources (bandwidth).

"Telecommunications" means the transmission of information, images, pictures, voice, or data by radio, video, or other electronic or impulse means.

Policy

Network access, to include the Internet, provides DMAVA with critical business advantages as a source of research and technical information, improved communication, public access and visibility, business and recruiting contacts, and electronic commerce. It is, therefore, in DMAVA's best interest to encourage prudent use of the network for State business purposes. The network presents employees with opportunities for easy, rapid and efficient global communications and research but also creates certain risks, including security risks, and legal liability. In order for the State to maximize the benefits and minimize the risks associated with use of the network, to include the Internet, this statement sets policy for network, to include Internet, access and use by all users whether authorized or unauthorized.

The only persons who may access the Internet through the DMAVA information infrastructure or information technology are DMAVA employees and such other persons as DMAVA may specifically authorize.

Employees are given DMAVA-provided access to the network to assist them in the performance of their jobs. DMAVA monitors network activity and therefore users should have no expectation of privacy. All records created by network use, including path records, are property of DMAVA, and are subject to monitoring. Users are expected to conduct their electronic communications in a professional, responsible, and courteous manner. Misuse of DMAVA's information infrastructure, information technology and electronic communications media, including, but not limited to, the unauthorized transmission of confidential or proprietary information; the use of profane, harassing or other offensive language; or other inappropriate uses, including, but, not limited to, those listed below, may subject the user to discipline, including termination of employment, initiation of civil action, or criminal prosecution.

The ability to access the network, to include the Internet, using DMAVA-provided software, hardware, information infrastructure, information technology and other facilities is governed by several existing State policies summarized below. In addition, the following Internet-specific policies must be followed to maintain a secure and harassment free work environment.

No Privacy Expectations

DMAVA reserves the right to access and disclose, for any purpose, the contents of any Internet messages sent to and from DMAVA's computer equipment, information infrastructure or information technology including e-mail, attachments to e-mail, and World Wide Web (www) browsing without prior notice. All users, including State employees, using the DMAVA-provided network waive any right to privacy in such messages, and consent to their being accessed and disclosed by DMAVA personnel. Users of the computers and computer network of DMAVA specifically authorize DMAVA to monitor, intercept, read, copy, or capture in any manner any information placed on this computer or computer system. DMAVA may disclose or use any information monitored, intercepted, read, copied, or captured to authorized personnel or law enforcement to be used for disciplinary or civil action or criminal prosecution.

The State may release or provide data or information if directed to do so by operation of law, pursuant to a lawfully issued subpoena, or pursuant to a ruling by a court or arbitrator of competent jurisdiction.

Nothing in this policy shall be taken to waive, relinquish or abrogate any privilege or confidentiality recognized by law or to authorize disclosure of any privileged, confidential or proprietary information except as provided by law.

DMAVA System Security

All employees shall ensure that their use of the network does not compromise the security and integrity of DMAVA's information infrastructure or information technology, networks and computer equipment, whether by allowing intruders into the networks or by introducing viruses or other threats.

Employees shall not use another employee's computer to gain access to the network without that employee's consent or supervisory approval. An employee shall not permit another person to access the Internet using the employee's computer, except as provided by the Department's policy. Users shall not share their network login information with anyone.

The DMAVA computing systems are unclassified systems. Classified information may not be processed, entered, or stored on a DMAVA computing system. Information is considered classified if it is Top Secret, Secret, and/or Confidential Information that requires safeguarding in the interest of National Security.

Users are to report any weaknesses in DMAVA computing system security, any incidents of possible misuse or violation of computer systems to the DMAVA Chief Information Officer.

Incident Response Handling

Upon identification of an incident, or suspected incident, the following actions must be taken: First, isolate the system by unplugging the network cable, but do not shutdown the system. Next, notify the Customer Support Center at 609-530-7177. The purpose is to compile supporting

evidence, impact assessments, associated costs; and effect containment, eradication and reconstruction measures necessary to effectively manage the breach.

Acceptable Use Policy

Employees are given access to the network through DMAVA information infrastructure and information technology to carry out DMAVA business. All State policies, including but not limited to the State's policies prohibiting harassment, work-place violence and sexual harassment, the Conflict of Interest Law and the agency code of ethics, apply to an employee's access or use of DMAVA information infrastructure and technology. Users must comply with all State and Federal laws and regulations applicable to the Internet and government network computer usage. Employees must adhere to the following conditions and/or restrictions regarding network access and use as set by DMAVA.

1. All data/information stored on DMAVA Computers and servers are the property of the State of New Jersey.

2. LAN/WAN resources are to be used by authorized users for business purposes only. They are not for personal use.

3. Installing software on a computer connected to DMAVA/GSN network is expressly prohibited without the written permission of the Chief Information Officer or designee.

4. Unauthorized software will not be used on DMAVA computers. All software used on State owned computers must be the legitimate property of the State of New Jersey and / or authorized for agency use in writing. Unauthorized or pirated software cannot be copied or used on any microcomputer. Software audits may be performed at any time. Employees who create, install, or use unauthorized, illegal, or unlicensed software may be subject to disciplinary action up to and including termination from State service.

5. Users will not run software applications (i.e. Firefox, Video Games, etc.) from a USB device, CD-ROM, or external hard drive in an effort to bypass network policies or security. .
6. Users are required to change network passwords every 90 days. Non-DMAVA network passwords should be changed based on the schedule set forth by the individual application and/or systems administrator policies (i.e. NCFS, MACS, PMIS, every 45 days, etc.).

7. A DMAVA network account will be automatically disabled after three consecutive unsuccessful login attempts, and the lockout recorded.

8. To ensure all data/files are backed up and secure, they must be stored on network file servers. DMAVA-IASD is not responsible for files saved on a local “C” drive. If an employee operates a standalone Computer (not connected to the network), it is his/her responsibility to ensure files are backed up and secure, except where agreed upon by the Chief Information Officer for security or operational requirements.

9. DMAVA creates and saves "disk images" of standard PC configurations. These images are used to repair problems and install or upgrade software. DMAVA-IASD reserves the right to re-image any agency computer at any time without prior notification.

10. The use of modems within DMAVA is restricted. Written approval from the Chief Information Officer or their designee is required for PC modem installation and/or modem access to any DMAVA computer system.

11. Users shall not divulge dialup modem phone numbers to anyone.

12. All computer hardware used for State business or located on State property must be the legitimate property of the State of New Jersey. Use of personally owned equipment on the DMAVA/GSN network is not permitted. Written approval of the agency Chief Information Officer or his/her designee is required for any exceptions to these policies.

13. All computer hardware purchased for business use by DMAVA employees is the legitimate property of the State of New Jersey. While responsibility for asset tracking is distributed across the Department, DMAVA-IASD has authority over the assignment and disposition of all computer equipment.

14. DMAVA-IASD is the primary office responsible for maintaining all DMAVA network infrastructure components (hubs, switches, and supporting UPS units) and all DMAVA agency servers, regardless of funding source.

15. At no time shall changes/modifications/additions be done to DMAVA/GSN network cabling, data jacks, wiring closets, or infrastructure without approval of the Chief Information Officer or his/her designee. No equipment shall be connected to cabling that has not been certified to be in compliance with industry standards by either an authorized cabling vendor or member of the IASD technical support staff.

16. Unauthorized access of, or attempts to gain unauthorized access to, any computer, records, data, databases or electronically stored information is prohibited.

17. Any user finding he/she has accessed an area of a system and/or file store to which he/she should not have access will immediately note the directory, menu or file information/name and location and notify the IASD Help Desk. If familiar with the menu, he/she should then exit that area of the system.

18. Passwords should never be stored in unprotected files or displayed on workstations. Users are responsible for maintaining password security. Never give your password to another user. Do not log onto the network under another users ID and password.

19. A Property Hand Receipt must be completed whenever any (IT) equipment is removed from DMAVA facilities. Long-term hand receipts will be utilized for assigned PDA's and laptops.

20. At no time should any computer or peripherals that are connected to DMAVA network be relocated or removed without prior authorization from appropriate directors and/or managers and the Chief Information Officer or his/her designee.

21. Any person discovering missing computer equipment shall immediately notify the IASD Help Desk and submit a written incident report to the agency Chief Information Officer.

22. Games are not permitted on DMAVA computers. If a user is aware of a game that is on his/her computer, the user should notify the IASD Help Desk immediately in order to have it removed. Use of games on DMAVA computers is a violation of department policy and is subject to appropriate disciplinary action.

23. The E-mail system is the property of the DMAVA and should be used for business purposes only. A more than incidental or occasional use of e-mail for non-work related purposes is not permitted. Incidental personal use may NOT include using the computer or email to view or to distribute items of a religious nature or any item, which would be in violation of the State or departmental policy prohibiting racial, gender, sexual, ethnic discrimination, and harassment in the workplace.

24. Users should be aware that electronic mail is inherently neither private nor secure.

25. E-mail is not to be used for the distribution of copyrighted, discriminatory, pornographic, religious, or other non-State business material.

26. E-mail may not be utilized at any time for advertising or political lobbying, or for the distribution of chain letters or jokes.

27. No user shall attempt to gain access to another's e-mail account without his/her authorization, except where specifically authorized by the Chief Information Officer for departmental business or investigative purposes.

Software for browsing the Internet is provided to users for State related business use only. As with the telephone, limited incidental personal use that does not interfere with work duties, that does not consume significant state resources, that does not constitute a use prohibited by this policy and that does not interfere with the activities of others are permitted by DMAVA. Personal use of DMAVA equipment shall not amount to more than occasional use and is to be limited to emaployees breaktimes, scheduled lunch break and/or off duty hours. More than limited incidental personal use may subject an employee to disciplinary actionand/ or removal of their Internet access. Incidental personal use of the Internet is subject to monitoring or interception like any other Internet use.

Examples of Impermissible Uses

The following are examples of impermissible uses of DMAVA information infrastructure or information technology systems. This list is by way of example and is not intended to be exhaustive or exclusive. A user may not:

- Violate or infringe on a recognized privilege or the right to privacy;
- Transmit defamatory, false, inaccurate, abusive, profane, threatening, racially offensive, or otherwise biased, discriminatory or illegal material;
- Violate agency or departmental regulations or policies prohibiting harassment, workplace violence or sexual harassment;
- Violate any local, state, or Federal law;
- Conduct personal, for profit business activity;
- Solicit for religious, political, charitable or other causes;
- Conduct any non-governmental related fund raising or public relations activities;
- Gain or attempt to gain unauthorized access to any computer, computer records, data, databases or electronically stored information;
- Violate trademark or copyright laws; including software violations
- Knowingly cause the transmission of a program, information, code or command, and as a result of such conduct, intentionally causes damage to a computer;
- Play games on the Internet or gamble.
- Engage in instant messaging, streaming media, or streaming video for non-work related purposes.
- No user shall utilize DMAVA owned or leased information infrastructure or information technology to access, download, print or store any information infrastructure files or services having sexually explicit content.

Monitoring of Site Access and System Use

DMAVA reserves the right to monitor site access by users and to review data downloaded from the Internet. DMAVA may also monitor access to the DMAVA information infrastructure and information technology system (including successful and failed login attempts and logouts); inbound and outbound file transfers, and sent and received e-mail messages. DMAVA may monitor, intercept, read, copy, or capture in any manner any information placed on its computers or computer systems. DMAVA may disclose or use any information monitored, intercepted, read, copied, or captured to authorized personnel or law enforcement in any disciplinary or civil action or criminal prosecution.

Software

The DMAVA Chief Information Officer (CIO) must approve all software used on the DMAVA segment of the Garden State Network (SGN).

Virus Scanning

All files downloaded to the network must be scanned for viruses, using virus detection software approved by the DMAVA CIO.

Representing DMAVA
Employees must exercise the same care in posting information to the Internet or sending official correspondence via the email system as they would with any external communication by the Department.

Proprietary and Confidential Information
Users shall maintain all proprietary and confidential information in confidence and shall not use the Internet or the DMAVA information infrastructure or technology to access, disclose or distribute such information in an unauthorized manner or attempt to do so.

Copyright
Users should not violate any of the copyright laws when accessing printing or disseminating materials found on the Internet.

Consent
Access or use of DMAVA furnished computers, network infrastructure or Internet facilities constitutes consent to this policy on Acceptable Use of the DMAVA/GSN network

Responsibilities

Employee

- Employees shall adhere to this agreement and follow all State and Departmental Information Technology policies and procedures.

- Employees will POWER OFF their computers at the end of each business day to conserve electricity.

Agency

- DMAVA may develop agency guidelines, procedures, and internal controls for monitoring compliance with this policy.

- DMAVA shall distribute this policy to agency employees, and provide referenced standards and guidelines, as required.

- DMAVA may discipline employees for violations of this policy or any standards or guidelines referenced.

- DMAVA may promote awareness of acceptable usage policy by training employees in the use of tools and programs to access both the network and the Internet.

- DMAVA shall immediately furnish their current employees copies of this notice, and shall furnish all new employees copies of this policy concurrent with authorizing them to use agency computers.

References

Title VII of the Civil Rights Act of 1964 (as amended)

Communications Decency Act of 1996

Privacy Act of 1974, 5 U.S.C. 552a

Law Against Discrimination Act, N.J.S.A. 10:5-1 et. seq.

Civil Service Act N.J.S.A. 11A:1-1 et. seq.

Identity Theft Prevention Act, N.J.S.A. 56:11-44

N.J.A.C. 4A:7-1.3

Governmental Code of Ethics/New Jersey Conflicts of Interest Law

Executive Order 49 (Issued April 17, 1996)

OIT Policy 09-07 - Acceptable Internet Usage, (issued 30 January 2009)

Department of State Letter 03-10-ST Managing Electronic Email: Guidelines and Best Practices

IT Circular 12-01-OIT Security Awareness Program Policy

IT Circular 12-02-OIT Portable Computing Use and Temporary Worksite Assignment Policy

Joint Circular 12-10-OIT Assignment and Use of State Owned Cellular Wireless Devices

Departmental Directive 25.2.3 Information Security Program

Departmental Directive 25.2.4 Safeguarding Confidential and Privacy Act – Protected Data
Departmental Directive 25.2.5 COOP/COG Policies & Guidelines for State Laptop Users

Departmental Directive 25.2.7 Social Media Policy

Departmental Directive 105.6 Assignment and Use of Wireless Communications Devices

New Jersey Department of Military and Veterans Affairs (DMAVA)

Computer Resources Acceptable Use Policy Agreement
(Revised 1 October , 2012)

Use of the DMAVA computing systems are with the understanding that such use serves as consent to monitoring of any type of use, including incidental and personal uses, whether authorized or unauthorized.

Any noncompliance with the requirements outlined in this agreement will constitute a violation of this policy, will be reported to the management of the DMAVA network and the State Information Security Officer, and can result in disciplinary action, as well as, short-term or permanent loss of access to DMAVA computing systems. Serious violations may result in civil or criminal prosecution.

I have read and understand this Computer Resources Acceptable Use Policy (dated 1 October 2012) for use of the DMAVA computing systems and facility and agree to abide by it.

Signature_____ Date: _____

_____ _____
Printed: First Name, M. Last Name Grade/Rank/Title

_____ _____
Organization Duty Phone