State of New Jersey
DEPARTMENT OF MILITARY AND VETERANS AFFAIRS
POST OFFICE BOX 340
TRENTON, NEW JERSEY 08625-0340

☆☆

JON S. CORZINE
Governor
Commander-in-Chief

GLENN K. RIETH
Major General
The Adjutant General

DEPARTMENTAL DIRECTIVE NO. 25.2.4 **28 July 2006**

SAFEGUARDING CONFIDENTIAL AND PRIVACY ACT - PROTECTED DATA

1. PURPOSE

The purpose of this policy is to set forth guidelines to ensure the safeguarding of confidential and Privacy Act - protected data within all New Jersey Department of Military and Veterans Affairs (DMAVA) locations and facilities.

2. APPLICABILITY

This policy applies to all state employees, contract employees, hourly employees, offices and agencies within the New Jersey Department of Military and Veterans Affairs (DMAVA) that handle, process, review, access or store confidential or Privacy Act - protected information.

3. REFERENCES

- Identity Theft Prevention Act, NJSA 56:11-44
- DoD Directive 5400.11 Department of Defense Privacy Program
- NJOIT Electronic Mail / Messaging Policy
- DMAVA Departmental Directive 230.05
- DMAVA Security Policies and Procedures Guide
- Privacy Act of 1974; 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA)

4. DEFINITIONS

a. Authentication: Electronic security measure designed to establish the identity and access permissions of a computer network user. Authentication is used for network access to help validate transmission, message, or originator, or as a means of verifying an individual's authorization to receive specific categories of information.

b. Chief Information Officer: Senior Information Technology official for the department.

c. Confidential Information: Any information of a private nature that is protected by law from public disclosure. This includes but is not limited to documents or electronic information that includes name, address, social security or other identifying numbers, date of birth, medical history, financial information, etc…

d. Department: means the New Jersey Department of Military and Veterans Affairs.

e. Employee: means all state employees of the Department or agency whether full-time or part-time, and whether in the career service, executive service, or unclassified service. This term includes contracted employees, hourly employees, and interns.

f. Employer means the Department of Military and Veterans Affairs.

g. Identity Theft: The act of impersonating another, by means of using the person's information, such as birth date, Social Security number, address, name, and bank account information. Identity theft occurs when somebody steals your name and other personal information for fraudulent purposes. Identity theft is a form of identity crime (where somebody uses a false identity to commit a crime).

h. Privacy Act-protected data: means any item, record, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

i. Password: means the secure alpha / numeric code that individuals enter with their User ID to access the computer network.

j. User ID: means the assigned logon name and/or text used by an individual to access the computer network.

k. Work site. For purposes of this policy, work site means the primary physical area of operations of an employee within department or agency, including buildings, grounds, offices, desks, filing cabinets, and computers provided by the State.

5. OBJECTIVE

a. To prevent the loss of confidential or Privacy Act – protected data that can be used by individuals in the commission of identity theft and to safeguard both electronic and hardcopy employee and client information maintained by the offices and agencies within the Department of Military and Veterans Affairs.

6. POLICY

a. Effective immediately, all employees are prohibited from removing any confidential or Privacy Act - protected information, either electronic or hardcopy, from their primary work site to alternate work sites, their home of record, or any other location outside of department facilities that is not specifically authorized in the official performance of their assigned duties. Individuals will take all physical security measures necessary to insure that confidential information is not compromised while in transit or outside of an official work site. Instances were exposure of confidential and /or Privacy Act-protected data could occur should be minimized to the greatest extent possible in the performance of required duties.

b. Department employees, managers and supervisors are further directed to insure that all confidential and /or Privacy Act – protected information is secured in a locked cabinet, office or secure work area during any extended period that an individual is away from their work area and at the end of each work day.

c. Group security policies are in place on the DMAVA network that require all users to authenticate each time they access the department's network resources. Passwords contain a minimum number of characters and character combinations as proscribed by the department's Network Administrator. Users are required to change their passwords at designated intervals and cannot repeat a password for a certain number of consecutive periods.

d. Users are again cautioned to take all appropriate measures to insure that their user ID's and passwords remain secure and are not compromised. The sharing of a personal logon ID and password is strictly prohibited, unless specifically authorized by the DMAVA Chief Information Officer. A group security policy is also in effect that will automatically log-off users that leave a computer workstation unattended for a designated period of time and will require the user to log back into the network. The electronic group security policies are implemented in order to protect department data and prevent unauthorized access to department computer resources.

e. In addition, per the current State of New Jersey, Office of Information and Technology (OIT) E-Mail and Messaging policy dated 09/01/98, "State Employees should not expect their e-mail / messaging communications to be private, and should not use State-provided e-mail messaging systems for confidential matters that are not intended for public disclosure. E-mail/messaging unless secure, should not contain confidential information." To further clarify this policy, please note the use of the DMAVA e-mail system to transmit confidential and/or Privacy Act-protected information is strictly prohibited.

f. All DMAVA state computer network users will continue to review, complete and sign the "Acceptable Use Statement for the State Area Network (GSN) and Department of Military and Veterans Affairs Computing Resources" (SEE ENCL 1) prior to being granted departmental network access.

g. Violations of this directive are subject to discipline up to and including termination as cited in DD 230.05

7. RESPONSIBILITIES

a. Employees are responsible to comply with all provisions of this policy.

b. Managers and Supervisors are responsible to implement measures to ensure the security of confidential and Privacy Act – protected records within their, divisions, agencies, offices and facilities.

c. Managers and Supervisors have the responsibility to ensure that all staff members and subordinates are aware of the policies contained within this directive.

d. All employees are required to promptly notify their immediate superior, should they detect any violation of these directives or any systemic weakness that needs correction. Supervisors should evaluate any such reports, document as necessary and interface with technical staff, or higher authority, to institute corrective action if warranted.

The proponent of this Directive is the Information and Administrative Services Division Users shall submit comments and suggested improvements directly to NJDMAVA, ATTN: Director, IASD, P.O. Box 340, Trenton, NJ 08625-0340.

OFFICIAL:

GLENN K. RIETH
Major General, NJARNG
The Adjutant General

DAVID S. SNEDEKER
Chief Information Officer
Acting Director, Information and
Administrative Services Division

DISTRIBUTION: A, A1, E, F

Acceptable Use Statement
For The
State Area Network (GSN) and
Dept. of Military and Veterans Affairs Computing Resources

The following document outlines guidelines for use of the computing systems and facilities located at or operated by the Dept. of Military and Veterans Affairs (DMAVA). The definition of DMAVA computing facilities will include any computer, server or network provided or supported by the state Network Control Center (NCC). Use of the computer facilities includes the use of data/programs stored on DMAVA computing systems, data/programs stored on magnetic tape, floppy disk, CD ROM or other storage media that is owned and maintained by the NCC. 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.

DMAVA accounts are to be used only for the purpose for which they are authorized and are not to be used for non-work related activities. Therefore, unauthorized use of DMAVA computing systems and facilities may constitute grounds for possible adverse action.

1. The DMAVA/GSN computing systems are unclassified systems. Therefore, 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, which requires safeguarding in the interest of National Security.

2. All users are responsible for protecting any information used and/or stored on/in their accounts. Consult the User Security Guide for guidelines on protecting your account and information using the standard system protection mechanisms http://www.nj.gov/military/cio/docs/Security_Policy&Procedures.pdf

3. Users are requested to report any weaknesses in DMAVA computer security, any incidents of possible misuse or violation of computer systems to the Help Desk or by sending electronic mail to the state Information Security Officer.

4. Users shall not attempt to access any data or programs contained on DMAVA/GSN systems for which they do not have authorization or explicit consent of the owner of the data/program.

5. Remote users (personnel utilizing laptops) will not access the internet using personal **Internet Service Providers**. When internet access is required it will done by dialing into the State network. This is the only authorized manner of internet access.

6. Users shall not divulge Dialup or Dialback modem phone numbers to anyone.

7. Users shall not share their DMAVA account(s) with anyone.

8. Users shall not make unauthorized copies of copyrighted software, except as permitted by law or by the owner of the copyright.

9. Users shall not make copies of system configuration files (e.g. /etc/password) for their own, unauthorized personal use or to provide to other people/users for unauthorized uses.

10. Users shall not purposely engage in activity with the intent to: harass other users; degrade the performance of systems; deprive an authorized user access; obtain extra resources, beyond those allocated; circumvent computer security measures or gain access to a DMAVA system for which proper authorization has not been given.

11. Electronic communication equipment is for authorized government use only. The access of pornographic, gambling or other inappropriate web sites is not authorized. Government e-mail will not be used for commercial business and/or the forwarding of chain letters. Fraudulent, harassing or obscene messages and/or materials shall not be sent from, to or stored on DMAVA systems.

12. Users shall not download, install or run security programs or utilities, which reveal weaknesses in the security of a system. For example, users shall not run password-cracking programs on DMAVA computing systems.

13. DMAVA computing systems will not be used at any time to further personal gain.

14. All workstations must remain **POWERED ON** at the end of each business day (exceptions will be made on a case by case basis). Individuals will only logoff as the user at the end of each day.

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 these requirements will constitute a security violation and will be reported to the management of the DMAVA network and the state Information Security Officer and can result in short-term or permanent loss of access to DMAVA computing systems. Serious violations may result in civil or criminal prosecution and other adverse actions.

I have read and understand this Acceptable Use Statement for use of the DMAVA computing systems and facility and agree to abide by it.

Signature_____ Date_____

_____ _____

Printed: First Name, Middle Initial, Last Name Grade/Rank

_____ _____

Organization Duty Phone