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 25.2.5 **1 August 2008**

COOP/COG POLICIES & GUIDELINES FOR STATE LAPTOP USERS (IASD-ISB)

1. PURPOSE: The purpose of this policy is to set forth Continuity of Operations, Continuity of Government (COOP/COG) guidelines for all New Jersey Department of Military and Veterans Affairs (DMAVA) laptop users.

2. APPLICABILITY: This Bulletin applies to all state and federal employees, contract employees, and hourly employees, from the offices and agencies within the New Jersey Department of Military and Veterans Affairs (DMAVA) regarding the use of individually assigned laptop computers.

3. REFERENCES:

a) HQDA Regulation 380-5 Department of the Army Information Security Program
b) DA PAM 25-1-1 Information Technology Support and Services
c) DMAVA Dept Dir 25.2.1 Information Security Program
d) DMAVA Dept Dir 25.2.4 Safeguarding of Confidential & Privacy Act - Protected Data
e) NJAC 13:45f NJ Identity Theft Act
f) DMAVA Dept Bulletin 01-08 Computer Resources Acceptable Use Policy
g) Treasury Circular OMB 98-15 Assignment of State-Owned Personal Computers to State Employees
h) DMAVA Security Policies and Procedures Guidelines

4. POLICY: State-owned laptop computers and peripheral equipment may be assigned to state employees for use away from assigned duty stations at temporary departmental and non-departmental work sites, employee residences, and other authorized travel locations under the conditions specified below.

a. A laptop computer may be permanently assigned to an employee for use when work assignments and official duties require offsite computer access and the employee has demonstrated the level of knowledge regarding the equipment justifying the assignment, and work has been assigned which requires the use of a laptop computer.

1. The employee is assigned a laptop computer under the guidelines of the Senior Executive Services.

2. A laptop computer is assigned as part of COOP/COG contingency plans because of the individual's duty assignment, or if the individual's job requirements consist of a mobility assignment and not a permanent work site and the employee's knowledge regarding the equipment justifies the assignment.

b. Under no circumstance may a personal laptop computer be assigned to an employee's residence merely for the employee's convenience nor shall the equipment be utilized for personal business.

c. Approvals. Permanent assignments for use at employee residences shall be approved by the agency head or designee. Permanent or temporary assignments to temporary work sites or temporary assignments to employee residences shall be approved, at a minimum, by the employee's division director and the Agency Chief Information Officer (CIO).

d. Recordkeeping. All equipment with an original cost of at least $1,000 must be included on the department's equipment inventory. However, only equipment costing more than $10,000 should be reported to the Bureau of Risk Management.

The following information should be included:

- Brand name and model number
- Employee(s) to whom it is assigned
- Location (if it is being used at various temporary work sites, indicate that the piece of equipment is a "floater")
- Estimated fair market value.

e. A Property Hand Receipt shall be completed when any laptop equipment is permanently or temporarily assigned for individual use and removed from state premises. The information contained on the document shall include, but should not be limited to, the following:

- Employee taking custody of the equipment
- Equipment description, including serial number and inventory identification number
- Division, Office, Agency and/or Duty Position
- Authorized approval signature(s) and date.

5. COOP/COG LAPTOP GUIDELINES: All employees who are permanently assigned a state-owned laptop computer for individual use will remove the laptop from the work site on a daily basis, or during any extended absence from the office as part of the department's COOP/COG operations plan. This action is necessary in order to provide equipment availability for key agency personnel at the designated department disaster recovery (DR) site in the event that the DMAVA Headquarters Complex becomes inaccessible due to a man-made or natural disaster and/or other declared state of emergency.

a. All Department of Military and Veterans Affairs (DMAVA) employees with permanently assigned laptops are responsible to insure that all sensitive information and personal identity data is secured at all times. When removing a laptop computer from a secure work location all employees will insure the following conditions and guidelines are followed.

- Staff members will insure that their equipment is secured at all times when off site. NEVER leave a laptop unattended (in the open). Laptop theft is a crime of opportunity. Always keep the laptop at your side.

- NEVER leave a laptop stored in a parked car in plain view. Once again, laptop theft is a crime of opportunity. Breaking a car window and grabbing a laptop takes all of about 4 seconds.

- ALWAYS store a laptop in the trunk when storing in a vehicle--and note the remaining risk. Store your laptop in the trunk if you must leave it with the car. Heed storage temperature warnings from the manufacturer if extremely hot/cold temperatures are expected. Also note that some high-profile laptop thefts have occurred even with the laptop in the trunk.

- NEVER leave a laptop in an accessible area, such as a community room, apartment, or hotel room, in plain sight. Always keep the laptop out of sight. If you have a safe (many hotel rooms offer this now) use it.

- If possible CARRY the laptop in a discrete bag/case, NOT readily-identifiable as a laptop bag. While cases/bags designed for laptops are convenient, they also broadcast to potential thieves that you are carrying a nice target.

- ALWAYS lock doors, and lock the laptop machine itself if possible. If this seems like common sense...it is. Yet many laptop owners think their laptops will never be stolen. All DMAVA laptop users are authorized to request a locking cable system for their laptops by contacting the state customer support center and supplying their make, model and service tag number along with a request for purchase of a cable lock system. This will help deter any would be thieves especially when traveling.

- ALWAYS password protect and/or encrypt critical, sensitive information. Encryption tools can dramatically slow a laptop's performance, so be careful and consider the need. One disadvantage to total-drive encryption (encrypting the entire hard drive) is often performance loss. A disadvantage to partial-drive encryption (encrypting only special folders/files/areas) is that sensitive data is often accidentally placed outside the encrypted area. The primary rule is DO NOT store unencrypted sensitive data or personal identity information (PII) on your laptop.

- All DMAVA laptop users with permanently assigned equipment may request the issue of a FIPS / HIPPA compliant secure USB storage devices up to 8GB for their personal use in order to store and transport any sensitive or personal identity data for use off site. This is the only current authorized storage method for PII and sensitive data.

- ALWAYS install your operating system's latest security updates. Being attacked from the network itself is an enormous risk in the Internet Age. Your laptop will automatically be updated with the latest OS security updates when joined to the DMAVA network. Users should insure that they connect to the DMAVA network to obtain security updates at a minimum of once every week.

- ALWAYS install anti-virus/anti-spyware software. Protect your laptop's integrity by installing software to detect and remove viruses and spyware. Examples include Norton Antivirus (by Symantec), Forefront (by Microsoft) and McAfee. All DMAVA laptops run a corporate/enterprise version of anti-virus/ anti-spyware. Your laptop will automatically be updated with the latest anti-virus definitions when joined to the DMAVA network. Users should insure that they connect to the network to obtain updates at a minimum of once every week.

- ALWAYS keep the shoulder strap on, or a strap wrapped around your arm, when travelling in crowds. Some laptop thefts occur as regular "muggings." As with a purse, keep the strap of your laptop carrying bag around your shoulder or looped around your arm for extra protection. This will also help prevent accidental loss or misplacement in a crowd
.
- ALWAYS be aware of your surroundings. For overall security, including your own personal safety, always pay close attention. Being absorbed in a book, cell phone call, personal music player, newspaper, or other distractions can give thieves significant opportunity to approach, study, and even strike. Look at the people around you occasionally. Be alert.

7. The Department of Military and Veterans Affairs (DMAVA) in conjunction with the NJ Office of Information Technology continues to work toward additional enterprise-wide security solutions for data encryption, remote access and disaster recovery operations. Security of personal identity information maintained by the offices and agencies of the State of New Jersey remains a primary security concern. As additional technologies and procedures become available, this office will provide further guidance and assistance to all DMAVA state network users.

8. Questions or inquiries concerning this bulletin should be addressed to the department's Chief Information Officer, Mr. David Snedeker at (609) 530-6727 or email David.Snedeker@njdmava.state.nj.us

OFFICIAL:

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

GLENN K. RIETH
Major General, NJARNG
The Adjutant General

DISTRIBUTION: A, A1, A2, B, D, E, F