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

CHRIS CHRISTIE
Governor
Commander-in-Chief

☆☆
GLENN K. RIETH
Major General
The Adjutant General

DEPARTMENTAL DIRECTIVE NO. 25.2.2 **15 September 2010**

GARDEN STATE NETWORK (GSN) DATA AND TELEPHONE SYSTEMS RECORDS REQUEST PROCEDURES (IASD)

1. **PURPOSE:** To outline procedures and guidelines for the request and release of digital files or information from the DMAVA segment of the GSN and Telecommunications systems records, in order to insure compliance with federal /state privacy and regulatory requirements.

2. **APPLICABILITY:** This Directive applies to all employees, contractors and/or outside vendors that use or access department state (GSN/DMAVA) network or telecommunications resources within the New Jersey Department of Military and Veterans Affairs (DMAVA).

3. **REFERENCES:**

a. The Privacy Act of 1974
b. Federal Wire Tap Act, 18 U.S.C. §2710 et seq,
c. Guidance on Privacy Act Implementations of Call Detail Programs, 54 FR 12290
d. The Computer Matching and Privacy Protection Act of 1988
Computer Matching and Privacy Protection Amendments of 1990
e. Safeguarding Against and Responding to the Breach of Personally Identifiable Information (May 22, 2007)
f. New Jersey Wiretap Act, N.J.S.A 2A:156A-1 et seq.
g. Identity Theft Prevention Act, N.J.S.A. 56:11-44
h. Executive Order 49 (Issued April 17, 1996)
i. OIT Policy 09-07 - Acceptable Internet Usage, (issued 30 January 2009)
j. Treasury Circular 98-15-OMB Assignment of State-Owned Personal Computers to State Employees
k. Treasury Circular 97-03-OTS Guidelines for Acceptable Internet Access & Use for NJ Government
l. Treasury Circular 97-02-OTS Internet Access and Use Policy for New Jersey Government
m. Departmental Directive 25.2.4 Safeguarding Confidential and Privacy Act – Protected Data

4. **DEFINITIONS:**

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

b. **Computing systems and facilities:** are defined as any computer, server, or network provided by or supported by the DMAVA Customer Support Center (CSC).

c. **Digital Files:** Digital files include documents, images, e-mail, Internet usage reports.

d. **Garden State network (GSN):** the State of New Jersey wide area network that services all NJ State agencies and offices on a statewide geographic basis.

e. **PBX:** Private branch exchange, an in-house telephone exchange (system) that serves a particular department, business, office or facility.

f. **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.

g. **State-provided:** means access to the Internet, email, data or voice network via computer networks or telecommunications systems 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.

h. **Telecommunications Systems Records:** All PBX, Voice Mail (Call Pilot), vendor based , VoiP, telephone call records or recordings for cellular or landline phone systems

i. **VoiP:** Voice over Internet protocol, process for communicating by telephone (voice) utilizing an existing data network.

5. **OBJECTIVE:** To standardize and document departmental procedures for requesting electronic data or telephone systems information on individual employees, contractors and/or vendors.

6. **RESPONSIBILITIES:**

a. **Chief of the Joint Staff (COJS):** is responsible for final approval on release of information on all requests for personal electronic data or telecommunications systems information for any employee, contractor or vendors outside of the veterans affairs operations and facilities.

b. **Chief Information Officer (CIO):** is responsible for managing, reviewing, and forwarding all requests for release of personal electronic data or telecommunications systems information to the Chief of the Joint staff and/or Deputy Commissioner for Veterans Affairs for final release approval .

c. **Chief Technology Officer (CTO):** Upon approval of the CIO the Chief technology Officer is responsible for accomplishing all personal requests for electronic data or telecommunications systems information in a secure method. The CTO will approve any request for release of information in the absence of the Chief Information officer.

d. **Deputy Commissioner for Veterans Affairs:** is responsible for final approval on release of information on all requests for personal electronic data or telecommunications systems information for any employee, contractor or vendors within the veterans affairs operations and facilities.

e. **Deputy Attorney General:** The Office of law and public Safety, Deputy Attorney General assigned to represent DMAVA is responsible to review subpoenas, warrants, non-routine Open Public Records Act (OPRA) and/or other litigation requests for electronic data prior to agency release.

e. **Division Directors:** will review, approve and submit all requests for release of personal electronic data or telecommunications systems information for any employee, contractor and /or vendor support personnel within their respective organizations.

e. **DMAVA Systems Administrator:** will research, secure and provide digital copy or alternative media for all agency electronic data requests.

f. **Human Resources:** will be consulted as required on request for release of any electronic data requests involving personnel actions or employment records.

d. **Managers and Supervisors:** are responsible to comply with all provisions of this directive.

7. **BACKGROUND:** Although data requests are made for a multitude of reasons, the procedures outlined in this bulletin are designed to ensure a single system of checks and balances to ensure data is released only to authorized individuals or entities with the consent of pertinent leadership. Requests included under this policy are:

- Suspected violations of the DMAVA Acceptable Use Policy
- Legal requirements including litigation holds on data
- File requests to ensure business continuity

8. **PROCEDURE:** All electronic data / telephone systems information requests must be in writing (e-mail or memorandum) and be endorsed by the pertinent division director or equivalent and then be submitted to the Chief Information Officer for action. In the absence of the CIO all requests will be reviewed by the Chief Technology Officer prior to forwarding to the COJS and/or DCVA for final release approval . At a minimum requests must contain the following information:

- Employee Name
- Type of request
- Reason for request (justification)
- Data being requested to include applicable date(s)

9. **GENERAL:** This Directive as well as additional Information Technology Departmental bulletins and policies can be found on the publications section of the Department website at: http://www.nj.gov/military/publications/index.html.

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

OFFICIAL:

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

GLENN K. RIETH
Major General, NJARNG
The Adjutant General

DISTRIBUTION: B, C, D, E, F