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

MICHAEL L. CUNNIFF
Brigadier General
Acting Adjutant General

DEPARTMENTAL DIRECTIVE NO. 25.2.6 **15 February 2012**

PHYSICAL SECURITY STANDARDS AND POLICIES FOR INFORMATION TECHNOLOGY (IT) RESTRICTED SPACE (IASD)

1. **PURPOSE:** To ensure that departmental information technology hardware and resources are protected by adequate physical security measures that prevent physical tampering, damage, theft, or unauthorized physical access.

2. **APPLICABILITY:** This Directive applies to all New Jersey Department of Military and Veterans Affairs (DMAVA) facilities, employees, contractors and/or outside vendors that require access to department state GSN/ DMAVA network or telecommunications resources. This includes but is not limited to equipment that stores, processes or transmits data that has been classified as sensitive, confidential or protected data.

3. **REFERENCES:**

a. Information Security Management Standard (ISMS), ISO27001 Section A.9
b. DMAVA Dept Dir 25.2.1 Information Security Program
c. DMAVA Dept Dir 25.2.4 Safeguarding of Confidential & Privacy Act - Protected Data
d. DMAVA Dept Bulletin 01-08 Computer Resources Acceptable Use Policy
e. Safeguarding Against and Responding to the Breach of Personally Identifiable Information PII (May 22, 2007)
f. Identity Theft Prevention Act, N.J.S.A. 56:11-44
g. NJAC 13:45f NJ Identity Theft Act
h. AR 190-13 The Army Physical Security Program
i. HQDA Regulation 380-5 Department of the Army Information Security Program
j. DA PAM 25-1-1 Information Technology Support and Services

4. **DEFINITIONS:**

a. **Access:** the ability to physically access areas containing information technology equipment.

b. **Chief Information Officer (CIO):** senior information technology official for the Department.

c. **Chief Information Security Officer (CISO):** senior technology staff member for (IT) Security within the Department.

d. **Chief Technology Officer (CTO):** Primary information technology operations staff member within the Department directly responsible to the CIO for overall (IT) Operations.

e. **Computing systems and (IT) facilities:** any computers, servers, switches, routers, telecommunications or network hardware within the Department.

f. **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.

g. **Department:** the NJ Department of Military and Veterans Affairs.

h. **Employee:** 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.

i. **Employer:** the NJ Department of Military and Veterans Affairs.

j. **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.

k. **Hardware:** all desktop and laptop personal computers, monitors, servers, routers, switches, storage devices, power supplies, and other network devices.

l. **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).

m. **Infrastructure:** all WAN and LAN circuits, fiber connections, data cabling, telecommunications wiring and points of demarcation from a telco provider.

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

o. **Personal Information:** 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.

p. **Privacy Act-Protected data:** 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.

q. **Sensitive Information:** any information of a sensitive nature that should be protected from public disclosure.

r. **System Administrator:** primary technical staff member responsible for overall operations and maintenance of the LAN / Wan network, Servers and Data Center operations.

s. **Unaccompanied Access:** access granted to a single individual to enter a restricted and/or controlled area without another individual in their presence.

t. **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 implementing physical security measures for all department information technology assets to prevent physical harm, unauthorized access, disaster, destruction, and/or theft of hardware or data. To reduce the Department's risk for loss of Personnel Identity Information (PII), Personal Health Information (PHI), other sensitive information and/or identity theft.

6. **POLICIES & PROCEDURES:**

a. **FACILITIES:**

1. Access to areas containing confidential or protected data information or critical network infrastructure will be physically restricted.

2. Restricted IT areas include data centers, computer rooms, telephone closets, network router and switch rooms, PBX / VoIP system rooms, and similar areas containing IT resources. All access to these restricted areas must be specifically authorized.

3. Entrances to restricted IT areas should utilize high security door locks and/or electronic access control with the capability of providing an audit trail. Biometric Systems are encouraged. Where locking mechanisms with keypads are used to access secure areas, entry codes shall be changed at least annually. When badge or card reader systems are employed to log access into and out of a secure facility, "piggybacking" of badge holders shall be prohibited. Computer Rooms should be monitored by CCTV cameras wherever possible.

4. Utilities access for computer and network resources should also be restricted to authorized personnel only. Emergency power will be provided to all critical systems (servers, telecommunications, data facilities, etc.) based on the determination of mission criticality by each agency. Data centers, telecom closets and key communications assets will have back-up uninterrupted power supplies (UPS) as well as connections to emergency power to insure continuous power.

5. Each computer room should have redundant access to power, cooling, and networks. There should be at least an 18" access floor to provide for air flow and cable management. Data centers / Computer rooms, telecommunications systems room, and MDF / IDF closets, should have air filtration. Rooms should have high ceilings to allow for heat dispersal.

6. Data centers / computer rooms, telecommunications systems room, and MDF / IDF closets should have temperature between 55 and 75 degrees Fahrenheit and a humidity of between 20 and 80 percent. Environmental sensors should log the temperature and humidity of the room and report it to the network operations Center (NCC) for monitoring and analysis.

7. There should be a Halon or other total flooding agent solution in place in each data center/computer room, telecommunications systems room or key MDF / IDF closet for fire prevention. There should be fire extinguishers located in each computer room.. There may be respirators in computer rooms.

There must not be wet pipe sprinkler systems installed in data center / computer rooms or telecommunications systems closets.

8. Restricted IT areas, data centers, computer rooms, telephone closets, network router and switch rooms, PBX / VoIP system rooms, and similar areas containing IT resources which do not meet the minimum standard of a high security door lock should request support for any critical upgrades to the access security, environmentals and fire suppression systems to meet minimum physical security, health and safety standards. Requests should be generated by submission of a DMAVA Form 104 Project Request to the CFMO-ID Installations Division. A copy of these requests should be forwarded to the DMAVA CISO to document remediation action for physical security violations.

9. Sensitive IT resources located in unsecured areas should be secured by alternate means to prevent physical tampering, damage, theft, or unauthorized physical access to confidential or protected data.

10. IT equipment must be marked with some form of identification that clearly indicates it is the property of the Department of Military and Veterans Affairs.

11. All equipment shall be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

12. Backup tapes that contain mission critical or sensitive information must be stored offsite and rotated per agency back-up recovery policies and procedures.

13. Physical access to records containing confidential or protected data, and storage of such records and data in locked facilities, storage areas or containers shall be restricted.

b. **PERSONNEL:**

1. The facility Chief Executive office (CEO), Superintendent or appropriate Director will designate, in writing, all key personnel within their organization authorized unaccompanied access to any (IT) restricted area within their facility. An access roster in letter format (See Appendix 1) will be prepared in triplicate, one posted on the inside of the IT or telecommunications closet, data center or other IT restricted area door, one copy will be maintained in the facilities physical security file, and one copy will be forwarded to the Chief Technology Officer (CTO) as of 1 January each year. This unaccompanied access control roster should be kept to the minimum staff necessary.

2. All authorized individuals in (IT) Restricted areas must wear an identification badge on their outer garments so that both the picture and information on the badge are clearly visible at all times.

3. All visitors will be controlled and screened. The number of visitors should be kept to a bare minimum. Vendors and service contract providers who require access will be accompanied at all times within IT restricted areas. Tours of these areas by non-departmental, state or federal government personnel are prohibited.

4. The DMAVA Form No. 25.2.6 (R) sign in/sign out sheet (See Appendix 2) is required for all escorted visitors. It will be posted on the inside of each door within an (IT) restricted access room, along with the unaccompanied access roster. At all times while inside secure facilities, unauthorized personnel shall be accompanied by authorized personnel. The Form No. 25.2.6 (R) access log shall be used to record the entrance and exit dates/times of all unauthorized personnel as well as the names of the authorized personnel accompanying them, the name of the company represented and purpose of visit.

5. Annual access review by the agency/facility will be conducted for personnel designated with unaccompanied access to restricted areas (i.e. maintenance, telecommunications, etc...). Access controls and environmental considerations of primary facilities housing critical information systems should be reviewed and tested at least annually. Physical security requirements for access and environmental considerations should be evaluated each time there is a related security incident, significant alteration to the facility layout, or significant change to equipment/systems located at the facility.

6. Security Awareness Training provided by the NJ Office of Information Technology will be completed annually on-line by staff through the NJ Portal Learning Management System (LMS) and reported by the Agency LMS coordinator to the CTO.

7. The CISO will insure that restricted IT areas, data centers, computer rooms, telephone closets, network router and switch rooms, PBX / VoIP system rooms, and similar areas containing IT resources are inspected on an annual basis for compliance with the minimum physical standards for secure access. Senior MIS staff at each facility will report compliance with annual physical security inspections at DMAVA facilities as of 1 January each year. Violations will be reported to the CISO, CTO and copies will be provided to the facility CEO or Superintendent of the respective facility. All facilities without MIS support staff assigned will be reviewed annually by DMAVA central operations (IT) Staff representatives for compliance with this policy.

8. Violations of this policy may result in appropriate disciplinary measures in accordance with Departmental Directive 230.05, under the Disciplinary and Corrective Action Table of Offenses and Penalties as published by the DMAVA Human Resources Division.

Any individual who suspects a violation of this policy may report it to the Chief Technology Officer at the Central Operations Help Desk Number (609) 530-7177.

7. RESPONSIBILITIES:

a. **Chief Information Officer (CIO):** The Chief Information Officer is responsible for promoting and supporting effective physical security standards for all agency Information Technology (IT) assets and has overall responsibility for review and approval of all department-wide guidance for Information Technology Physical Security policies.

b. **Chief Technology Officer (CTO):** The Chief Technology Officer is responsible developing, reviewing, and publishing department-wide guidance for Information Technology Physical Security policies within the Department. . The CTO will approve any request for exemption from policy in the absence of the Chief Information Officer.

c. **Chief Information Security Officer (CISO):** The Chief Information Security Officer is the primary individual responsible for developing, implementing and insuring compliance with Information Technology Physical Security policies within the Department.

d. **Division Directors / Chief Executive Officers (CEO)/ Facility Superintendents:** will insure compliance with all policies and procedures contained with this Departmental Directive by personnel within their respective organizations and facilities. CEO's, Directors and Superintendents will submit a roster of individuals authorized unaccompanied access to (IT) restricted areas on an annual basis to the office of the Chief Information Officer for their respective facilities.

e. **Systems Administrator**: will review systems security and provide notice of any system security incidents and/or breaches to the CISO for investigation and remediation. The systems administrator shall

provide input to the CTO for any new or revised construction of existing data centers and or MDF / IDF construction, and will keep him informed of any environmental concerns

f. **Managers and Supervisors**: are responsible to comply with all provisions of this directive and to ensure that all staff members and subordinates are familiar with the policies contained within this directive.

g. **Employees**: are responsible to comply with all provisions of this policy. All employees are required to promptly notify their immediate superior, should they detect any violation of this 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.

8. **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.

Appendix 1: Sample Unaccompanied Access Letter
Appendix 2: Restricted (IT) Area Access Form

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:

MICHAEL L. CUNNIFF
Brigadier General, NJANG
Acting Adjutant General

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

DISTRIBUTION: A, B, D, E, F

Figure 1

FACILITY LETTERHEAD

15 February 2012

MEMORANDUM FOR RECORD

SUBJECT: Unaccompanied Access Roster

1. The following individuals are authorized unaccompanied access to the following Information Technology (IT) restricted areas within the: HQ's NJ Department of Military & Veterans Affairs BLDG # 101 , ROOM # _PBX Switch Basement_

NAME TITLE / RANK SSN (last three)

JOHN Q. PUBLIC	MIS MANAGER	X001
JANE DOE	FACIILITY ENGINEER	X002

2. The above listed personnel have been screened and approved by the facility CEO / Superintendant / Division Director and/or his designated representative IAW Departmental Directive 25.2. 6.

3. POC telephone numbers are DUTY HOURS: 609- 530-XXXX
AFTER DUTY HOURS: 609-209-XXXX

NAME
TITLE
OFFICE / LOCATION

Appendix 1

Figure 2

(IT) RESTRICTED AREA ACCESS SIGN-IN SHEET	
Facility:	Building No:
Address:	Place /Room:

Visitor Name	Company	Authorized Staff Escort Name	Date/time In	Date/time Out	Reason

DMAVA Form 25.2.6 (R), dated 10 Jan 2012