

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
The Adjutant General

DEPARTMENTAL DIRECTIVE

NO.

25.2.9

15 September 2016

INFORMATION ASSURANCE - AUTHORITY TO OPERATE SYSTEM ADMINISTRATOR SECURITY POLICY (IASD)

1. PURPOSE

The purpose of this policy is to implement Information Assurance industry standards and regulatory guidance for Systems Administrator access for all computer systems and applications accessed and utilized within all New Jersey Department of Military and Veterans Affairs (DMAVA) locations and facilities to ensure the safeguarding of confidential and sensitive data in order to meet inter-agency security requirements for Authority to Operate (ATO) for electronic exchange of confidential data.

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 access the New Jersey Department of Military and Veterans Affairs (DMAVA) and Garden State Network (GSN) network and enterprise applications.

3. REFERENCES

- DOD Directive 8570 Information Assurance Compliance and Certification
- DOD Directive 8500.1, Information Assurance
- DOD Directive 8500.2, Information Assurance Implementation
- DOD Regulation 5200.1 Information Security Program
- National Institute of Standards and Technology (NIST) Special Pub (SP) 800-12
- National Institute of Standards and Technology (NIST) Special Pub (SP) 800-53
- ISO/IEC 27002:2005 Information Security Management

- ISO/IEC 27002:2013 Information Security Management
- State of New Jersey. N.J.S.A. 52:18a-230 b
- Treasury Circular 14-08-NJOIT 180 - Security in Application Development Policy
- Treasury Circular 14-18-NJOIT 174 – Network Security Policy
- Treasury Circular 14-13-NJOIT 205 – Certification and Accreditation Policy
- Treasury Circular 14-29-NJOIT 172 – Access Control Management Policy
- DMAVA Dept Dir 25.2.1 Information Security Program
- DMAVA Dept Dir 25.2.4 Safeguarding of Confidential & Privacy Act - Protected Data
- DMAVA Departmental Directive 230.05
- Identity Theft Prevention Act, NJSA 56:11-44
- NJAC 13:45f NJ Identity Theft Act
- Privacy Act OF 1974; 5 U.S.C. § 552a
- Health Insurance Portability and Accountability Act (HIPAA)

4. DEFINITIONS

a. Accreditation: Formal declaration by a Designated Accrediting Authority (DAA) or Principal Accrediting Authority (PAA) that an information system is approved to operate at an acceptable level of risk, based on the implementation of an approved set of technical, managerial, and procedural safeguards.

b. 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.

c. Authorization to Operate (ATO): An Authorization to Operate (ATO) is a formal declaration by a Designated Approving Authority (DAA) that authorizes operation on a network. The ATO is signed after a Certification Agent (CA) certifies that the system has met and passed all security requirements to become operational.

d. Certification: Comprehensive evaluation of the technical and non-technical security safeguards of an information system to support the accreditation process that establishes the extent to which a particular design and implementation meets a set of specified security requirements.

e. Chief Information Officer (CIO): Senior Information Technology official for 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: means the New Jersey Department of Military and Veterans Affairs.

h. 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.

i. Employer: means the Department of Military and Veterans Affairs.

j. 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).

k. Information Assurance (IA): Information Assurance (IA) refers to the steps involved in protecting information systems, like computer systems and networks. Measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

l. Information Security (INFOSEC): sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, inspection, recording or destruction. It is a general term that can be used regardless of the form the data may take (e.g. electronic, physical).

m. Memorandum of Agreement (MOA): (MOA) is a written document describing a cooperative relationship between two parties wishing to work together on a project or to meet an agreed upon objective. An MOA serves as a legal document and describes the terms and details of the partnership agreement.

n. Network Administrator: A network administrator is an IT expert who manages an organization's network. The network administrator must possess a high level of technological knowledge and is most commonly the highest level of technical staff within a given organization.

o. 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.

p. SA Account: is a systems administrator account with separate access and elevated privileges that provide ability to change network systems, applications and data with little or no restriction.

q. Systems Administrator (SA): or sysadmin, is a person who is responsible for the upkeep, configuration, and reliable operation of computer systems, local and wide area networks, servers, and enterprise applications.

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

s. 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 implement and insure compliance all legal and regulatory Information Assurance standards and policies required under published federal and state guidelines with the Department.

b. To secure all internal and external enterprise and local computer network applications and systems to prevent data breach, loss of data, corruption and/or catastrophic failure of confidential systems and data to insure regulatory compliance for information assurance requirements and agency accreditation and certification for inter-agency digital information exchange Authority to Operate.

c. To secure and protect the integrity of all employee and client information and electronic data maintained by the offices and agencies within the Department of Military and Veterans Affairs, IAW current industry Information Security standards.

6. POLICY

a. Effective immediately, only designated Information Technology (IT) staff with appropriate training and/or certifications will have Systems Administrator (SA) privileges within any enterprise network systems and/or applications within the Department of Military and Veterans Affairs (DMAVA). In addition, all SA privileges will be limited in scope for staff to those required to fulfill their (IT) Support functions within their range of duties and location. Systems Administrator (SA) must maintain their training and/or certifications at the appropriate level in order to retain their Systems Administrator account access. The use of SA or elevated privilege accounts and permissions will be minimized to the greatest extent possible in the performance of required duties.

b. All other Department staff will need to request any enterprise systems or application changes, network actions or systems modifications through the normal Help Desk / Customer Support ticketing process through the Central Operations Help Desk in Lawrenceville or the resident MIS Manager at each Veterans Memorial Home facility as appropriate. All requests will be assigned a Help Desk ticket number and be prioritized and assigned to the appropriate Systems Administrator for action. Please note this does not include local database programs or spreadsheet or other applications like Microsoft Access, Microsoft Excel, etc., which are created and maintained by our end users.

c. All Department Information Technology staff will be required to establish and use a separate logon account for Systems Administrator (SA) activities and duties, known as an SA Account. This account will not be used as the individual's regular logon to perform routine tasks or work requirements that do not require elevated systems privileges such as drafting letters, correspondence , email, procurements actions, time and attendance, etc.

d. 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. SA Account users will be subject to a more stringent password policy and will be required to change their passwords at shorter intervals and cannot repeat a password for a longer number of consecutive periods.

e. This policy action is implemented as a regulatory requirement in order to establish Accreditation and Certification with federal organizations and other state agencies in order to meet current minimum Information Assurance requirements for an Authority to Operate on their network and/or to exchange or accept confidential and sensitive electronic information within our network. The US Dept of Veterans Affairs and the Defense Management Data Center (DMDC) require compliance with all federal and state legal and regulatory electronic information security standards and policies in order to maintain our Authority to Operate (ATO) with the Designated Accrediting Authority (DAA) . The electronic group security policies being implemented are in order to protect Department data and prevent unauthorized access, loss or damage to Department computer resources and systems.

f. Staff from the New Jersey Department of Military and Veterans Affairs (DMAVA) Information and Technology operation for the agency are prohibited from granting Systems Administrator and/or elevated privileges for any network system or enterprise application even on a temporary basis. This is in direct violation of all current state and federal regulatory guidelines and will be consider a violation of best practice policies with our agency.

g. All DMAVA state computer network users including those (IT) Staff with SA Accounts 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" on an annual basis prior to being granted departmental network access. In addition, Systems Administrators (SA) will also be required to sign a non-disclosure agreement.

h. 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 ensure staff compliance with this directive and promote Information Security throughout their organizations to assist in protecting confidential and sensitive data and systems within the Department.

c. The IT Staff within the Department of Military and Veterans Affairs (DMAVA) is responsible for implementing this Information Assurance policy, insuring agency compliance by all end users, and managing all network assets and technical information security requirements to support this action.

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.

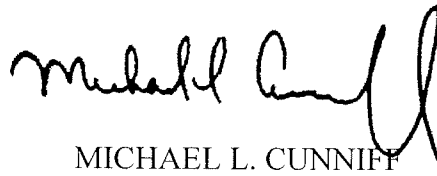
The proponent of this Directive is the Information and Administrative Services Division (IASD).

Users are invited to submit comments and suggested improvements directly to
NJDMAVA, ATTN: IASD, 101 Eggerts Crossing Road, Lawrenceville, NJ 08648.

OFFICIAL:



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



MICHAEL L. CUNNIFF
Brigadier General, NJANG
The Adjutant General

DISTRIBUTION: A, B, C, D, E, F