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. 25.2.8

15 December 2013

AGENCY PASSWORD POLICIES AND STANDARDS FOR DMAVA STATE NETWORK ACCOUNT USERS (IASD)

1. **PURPOSE:** The purpose of this policy is to identify and establish the requirements for password construction, protection, storage, and management for the NJ Department of Military and Veterans Affairs (DMAVA) state network. The issuance of this standard is to minimize the potential exposure to New Jersey's computers, network systems and infrastructure from unauthorized access, loss of sensitive or confidential information, and/or damage.

2. **APPLICABILITY:** This Directive applies to all state and federal agency employees, contractors, business partners, consultants, temporary employees, and others who develop, administer, maintain, and/or access information systems or software applications, that reside on the departments DMAVA state network. 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) State of New Jersey Circular 13-11-NJOIT, 177- Password Management Policy
   b) State of New Jersey Circular 13-11-S1-NJOIT, 177-01 Password Management Standard
   c) State of New Jersey Circular 12-03-NJOIT,110 - Security Framework Policy
   d) Information Security Management Standard (ISMS), ISO 27001
   e) National Institute of Standards and Technology (NIST), SP 800-118
   f) DMAVA Dept Dir 25.2.1 Information Security Program
   g) DMAVA Dept Dir 25.2.4 Safeguarding of Confidential & Privacy Act - Protected Data
   h) DMAVA - Computer Resources Acceptable Use Policy (annual Departmental Bulletin)
   i) Identity Theft Prevention Act, N.J.S.A. 56:11-44
   j) NJAC 13:45f NJ Identity Theft Act
   k) State of New Jersey Public Law P.L.2007.c.56

4. **OBJECTIVE:** To ensure the protection of information assets and establish the minimum requirements for password management and standards to ensure that all departmental state computers, network systems and infrastructure comply with State and Federal laws for securing confidential, proprietary, and/or sensitive information.

5. **POLICY:**

a) User Authentication & System Access

For access to any Department of Military and Veterans Affairs State Government information computer system or infrastructure, authorized users must create and supply their individual password as a means of authentication. The construction of a password must conform to the rules and standards specified this document.

b) Affected Systems & Applications

Passwords are required for all computers, systems and infrastructure owned and/or operated by the State of New Jersey and all platforms (operating systems) and applications systems, web-based applications, workstations, network devices, databases, directories, and any programs developed by staff, and/or third-party purchased software, etc…

c) Password Selection

All user-chosen passwords must contain a sufficient level of complexity created by using four of the four categories of: lowercase letters, uppercase letters, digits, and symbols. The use of control characters and other nonprinting characters is prohibited. Automatic system notices will be implemented to enable all users to change their passwords as appropriate.

d) Password Constraints

The display and printing of passwords shall be masked or obscured so that unauthorized parties will not be able to observe or subsequently recover them. After three unsuccessful attempts to enter a password, the involved USER/ID must be either; (a) suspended until reset by a system administrator, (b) if a dial-up or other external network connection is involved, it will be disconnected.

e) Password Sharing

All passwords are to be treated as sensitive and confidential information. All staff responsible for account creation and maintenance are prohibited from sharing user’s passwords and/or USER/IDs with other users, except for the authorized purpose of making changes and/or revoking accounts or passwords. The sharing of passwords with any person is prohibited.

6. STANDARDS & PROCEDURES:

Password requirements of this standard will be satisfied either through the management of the security functions or through technical features.

a) Password Construction/Selection

1) Individuals that access state network systems or applications must have passwords at least ***eight (8)*** characters in length.

2) Passwords must include ***at least four (4)*** combinations of letters, numbers, punctuations, and special characters, (e.g., a-z, A-Z, 0-9 ~ `! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ]:" ;' < > ? , . /)

3) Passwords cannot be a word in any language, slang, dialect, jargon, etc.

4) Passwords will not be inserted into email messages or other forms of electronic communications.

5) Passwords cannot contain any parts of your USER/ID, suggest to, or contain user privileges.

6) Null (blank) passwords shall be prohibited.

b) Password Protection

1) Privileged user accounts such as System Admin or data owners will have different USER/IDs and passwords to perform administrative functions, which are distinct and separate from their individual user accounts.

2) All USER/IDs that are **not** assigned to an individual user (operating systems, applications, or other) will be deleted and/or disabled, to minimize excess systems maintenance for password changes, etc.

3) User account lockout feature shall disable the user account after 3 unsuccessful login attempts.

4) User account lockout duration shall be permanent until an authorized system administrator reinstates ***(unlocks)*** the user account.

5) The following items make for good password security and are to be followed:

   - Never reveal your passwords to anyone or share them over the phone.
   - Never share passwords with co-workers while you are out of the office or on vacation.
   - Never talk about your password in front of others.
   - Never hint at the format of a password (e.g., "my family name").
   - Never reveal a password on questionnaires or security forms.
   - Do not select to auto save passwords or the "Remember Password" feature of applications (i.e. Eudora, Outlook, Internet Explorer, etc…).
   - Do not use the same password for business that you use for non-business purposes.

6) If an account or password is suspected of having been compromised, the incident shall be immediately reported to the appropriate supervisor and local agency Help Desk. The Help Desk shall report the incident to the appropriate IT/Security staff. The IT/Security Manager

will assist with investigating all incidents involving compromised passwords or suspected security violations involving passwords.

c) **Password Storage**

Passwords shall not be stored in a readable format without access controls, nor placed in any location where unauthorized persons may discover them.

d) **Password Changes & New Passwords**

1) Passwords shall be changed on a regular rotational basis; a system generated reminder should prompt users at least every ninety (90) days to change their passwords.

2) Privileged user accounts such as IT administrators or data owners with administrative access should have their password changed at least every sixty (60) days.

3) Passwords must have at least a 15-day minimum age with exceptions for privileged users and/or system constraints.

4) Passwords must be promptly changed if suspected of disclosure, or known to have been disclosed to an unauthorized party.

5) In the event that a user is locked out of the system or requires administrative assistance to change their password, that user must present suitable identification, such as USER/ID, current password, etc., to the appropriate authorized security personnel.

6) User accounts and passwords shall be systematically disabled after 90 days of inactivity.

7) Network operating systems shall routinely prompt users to change their passwords within 5-14 days before such passwords expire.

8) Users' passwords shall be prohibited from re-using their last six passwords.

9) Users shall be prohibited from changing their passwords for at least 15 days after a recent change. Meaning, the minimum password age limit shall be 15 days after a recent password change.

10) Passwords shall not be automated through function keys, scripts or other methods where passwords may be stored on the system.

7. RESPONSIBILITIES:

a) Agency Chief Information Officers & IT Directors

1) Provide for the distribution of this statewide policy within departments/agencies.

2) Ensure that Agency personnel are aware of and utilizing the appropriate user education training classes as they become available.

3) Inform all Agency employees/users of this policy.

4) Exercise the appropriate procedures for handling the security of user accounts and passwords, including resolution of security incidents.

b) **Network & Systems Administrators**

1) Exercise the appropriate procedures for handling user accounts and passwords, including resolution of security incidents.
2) Maintain separate and distinct USER/IDs and passwords for system administration and individual accounts.

c.) **Employees & Users**

1) Must review and adhere to this policy.
2) Report all incidents with passwords to the appropriate personnel.

8. **EXCEPTIONS AND COMPLIANCE**

This policy will be effective 20 Days from its publication, at that time all state network users will be required to reset current passwords for compliance.

A compliance exception must be requested in writing if there is an inability to comply with any portion of this policy. Exceptions and non-compliance shall be managed in accordance with Enterprise Policy 07-2004 Information Security Managing Exceptions.

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

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