NJ OFFICE OF INFORMATION TECHNOLOGY
Chris Christie, Governor
Dave Weinstein, Chief Technology Officer

P.O. Box 212
300 Riverview Plaza
Trenton, NJ 08625-0212

www.tech.nj.gov

STATE OF NEW JERSEY TECHNOLOGY CIRCULAR 177-01 – Password Management Standard	**POLICY NO:** 14-32-S1-NJOIT	
	SUPERSEDES: 13-11-S1-NJOIT	**EFFECTIVE DATE:** 10/14/2014
	VERSION: 1.0	**LAST REVIEWED:** 10/14/2014

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

This standard promulgates a compulsory set of technologies, metrics, configurations, and/or specifications to be uniformly applied across the State of New Jersey Executive Branch of State Government. This standard ensures that all State of New Jersey enterprise systems comply with State and Federal laws for the security of confidential, proprietary, and/or sensitive information.

2 AUTHORITY

This policy is established under the authority of the State of New Jersey. N.J.S.A. 52:18a-230 b. This policy defines New Jersey Office of Information Technology's (NJOIT) role with regard to technology within the Executive Branch community of State Government.

The New Jersey Office of Information Technology (NJOIT) reserves the right to change or amend this circular.

3 SCOPE

This standard applies to employees, contractors, business partners, consultants, temporary employees, and others who develop, administer, and maintain information systems, networks, software applications, and resources for New Jersey State Government, the Office of Information Technology, and/or their client.

4 STANDARD (IMPLEMENTATION)

Password requirements of this standard may be satisfied either through the management of the security functions or through technical features. This standard does not specify how the criteria shall be met, but only what criteria shall be met.

4.1 Password Construction/Selection

4.1.1 Staff must have passwords at least ***eight*** characters in length.

4.1.2 Systems should have a password policy module to control length, complexity and lifecycle. Passwords must include a combination of at least two of the following categories:

4.1.2.1 Uppercase (A through Z).

4.1.2.2 Lowercase (a through z).

4.1.2.3 Numbers (0 through 9).

*4.1.2.4 Punctuations and special characters, (e.g., ! @ # $ % ^ & * ( ) _ + | ~ - = \ ` { } [ ]:";' < > ? , . /).*

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

4.1.4 Passwords that protect information in an electronic communication cannot be included in that communication. Passwords that are themselves encrypted or protected in some other way are the only exceptions. Example: An encrypted email should not also contain the password that grants access to the encrypted communication. Clear text passwords (unencrypted plain text) cannot be inserted into email messages or other forms of electronic communications with the protected information.

4.1.5 Passwords cannot contain any parts of your USER/ID, or contain user privileges.

4.1.6 The use of ASCII or Unicode non-printing characters is prohibited.

4.2 Password Protection

4.2.1 Privileged user accounts such as those of IT administrators or data owners will have different USER/IDs and passwords to perform administrative functions, which are distinct and separate from their individual user accounts.

4.2.2 With present exceptions, all USER/IDs assigned to an operating systems service, applications, or other, must be managed by an individual and supervisor, or will be deleted and/or disabled to minimize excess system maintenance for password changes.

4.2.3 User account lockout feature shall disable the user account after three (3) unsuccessful login attempts. The information system must limit the number of consecutive unsuccessful access attempts allowed in a specified period and

automatically perform a specific function (e.g., account lockout, delayed logon) once the maximum number of attempts is exceeded.

4.2.4 User account lockout duration shall be permanent until an authorized System Administrator reinstates the user account.

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

4.2.5.1 Never reveal your passwords to anyone.

4.2.5.2 Never share passwords with co-workers.

4.2.5.3 Never talk about your password with others, nor document it in writing.

4.2.5.4 Never hint at the format of a password (e.g., "my family name").

4.2.5.5 Never reveal a password on questionnaires or security forms.

4.2.5.6 Do not select to auto save your password or the "Remember Password" feature of applications (e.g., Eudora, Outlook, Internet Explorer, and Netscape Messenger, etc.).

4.2.5.7 Do not use the same password for business that you use for non-business purposes.

4.2.6 If an account or password is suspected of having been compromised, the incident shall be immediately reported to the appropriate supervisor and Help Desk. The Help Desk shall report the incident to the appropriate MIS/Security staff. The MIS/Security staff will assist with changing all passwords.

4.3 Password Sharing

4.3.1 All passwords are to be treated as sensitive and confidential State of New Jersey information. All staff members responsible for account creation and maintenance are prohibited from sharing user passwords and/or USER/IDs with unauthorized personnel. System administrators are not authorized to grant privilege access to anyone without the written consent of an agency IT director, IT supervisor or department designee.

4.3.2 Sharing of passwords with any person is prohibited. Senior-level management (e.g. Commissioner, Assistant Commissioner, and other senior management) may allow viewing of their email accounts and/or calendars. This access should be provided without the sharing of passwords.

4.4 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.

4.4.1 Password Changes & New Passwords

4.4.1.1 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.

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

4.4.1.3 User Accounts are to be systematically disabled after 90 days of inactivity. Passwords must have at least a 15-day minimum age with exceptions for privileged users and/or system constraints.

4.4.1.4 Previously used passwords will not be accepted if a user account has been compromised or if there is suspicion that a password has been disclosed to an unauthorized party.

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

4.4.1.6 Information systems shall routinely prompt users to change their passwords within five to 14 days before such passwords expire.

4.4.1.7 When changing a password, users shall be prohibited from using their last six passwords.

4.4.1.8 Users shall be prohibited from changing their passwords for at least 15 days after a recent change, but the help desk can rest a password at any time if warranted.

4.4.1.9 Passwords shall not be automated through function keys, scripts or other methods that allows passwords to be stored on the system, except where such automation is required or mandatory for the functionality of an application and/or services. A compliance exception must be filed and approved.

5 MAINTENANCE

5.1 Password Audit Trail

5.1.1 The audit trail shall capture all successful login and logoff attempts.

5.1.2 The audit trail shall capture all unsuccessful login and authorization attempts.

5.1.3 The audit trail shall capture all identification and authentication attempts.

5.1.4 The audit trail shall be protected from unauthorized access, use of deletion or modification.

6 EXCEPTIONS AND NON-COMPLIANCE

Departments and Agencies shall comply with this policy within 90 days of its effective date.

A compliance exception must be requested 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 08-2002, Information Security Managing Exceptions.

Signature on File *10/14/2014*

E. STEVEN EMANUEL **DATE**
Chief Technology Officer-NJ Office of Information Technology
State Chief Information Officer