NJ OFFICE OF INFORMATION TECHNOLOGY
Philip D. Murphy, Governor
Odysseus Marcopolus, Chief Operating Officer

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

www.tech.nj.gov

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

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to identify and establish the requirements for password construction, protection and storage for the Executive Branch of New Jersey State Government. This policy is intended to compel compliance with State and Federal laws for the security of confidential, proprietary, and/or sensitive information as they relate to computer systems and infrastructure.

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 policy applies to employees, contractors, business partners, consultants, temporary employees, and others who access, develop, administer and maintain information systems, networks, software applications, and resources for New Jersey State Government, the Office of Information Technology, and/or their clients. It also applies to sensitive information.

4 POLICY

To ensure the protection of information assets, the minimum requirements for password construction, protection, storage, and changes shall be:

4.1 User Authentication and System Access

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

4.2 Affected Systems and Applications

Passwords are required to gain access to 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 programs.

4.3 Password Selection

All user-chosen passwords must contain a sufficient level of complexity created by using symbols from at least three of four groups: lowercase letters, uppercase letters, numbers, and symbols. Passwords using control characters and other nonprinting characters (ESC \e, DEL ^?, NULL \0) are prohibited. Automatic system notices should be implemented to remind all users to change their passwords when appropriate.

4.4 Password Constraints

The display and printing of passwords shall be masked, suppressed, or obscured. After three unsuccessful attempts to enter a password, a USER/ID must be:

4.4.1 Suspended until reset by a system administrator.

4.4.2 Disabled temporarily until resubmission is authorized by a systems administrator, or

4.4.3 Disconnected if a dial-up or other external network connection is involved.

5 RESPONSIBILITIES

5.1 Departments and Agencies

5.1.1 Provide for the distribution of this policy within Departments/Agencies.

5.1.2 Ensure that Departments/Agencies are aware of and utilizing the appropriate user education training classes as they become available.

5.1.3 Inform all employees/users of this policy.

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

5.2 Network & Systems Administrators

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

5.2.2 Maintain separate and distinct USER/IDs and passwords for system administration and individual accounts.

5.3 Employees and Users

5.3.1 Review and adhere to this policy.

5.3.2 Report all incidents with passwords to the appropriate personnel.

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.