NJ Office of Information Technology
Chris Christie, Governor
E. Steven Emanuel, Chief Technology Officer

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

www.nj.gov/it/ps/

STATE OF NEW JERSEY IT CIRCULAR

Title: 1701 – Identification and Authentication Policy

NO:	SUPERSEDES:
14-27-NJOIT	N/A
LAST REVIEWED: October 24, 2014	**DATE PUBLISHED:** October 24, 2014
VERSION: 1.0	**EFFECTIVE DATE:** Date of Signature
FOR INFORMATION CONTACT: Office of Policy and Planning	

ATTN: Directors of Administration and Agency IT Managers

I. PURPOSE

The purpose of this document is to establish a policy ensuring identification and authentication controls are in place for State Information Technology systems and networks, and that the methodologies for authorizing and authenticating access to the Executive Branch of State Government's infrastructure, devices, and services are in accordance with local, state, and federal regulations.

II. 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.

III. SCOPE/APPLICABILITY

This policy applies to employees, contractors, 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 their clients.

IV. DEFINITIONS

Please refer to the Statewide Policy Glossary at http://www.nj.gov/it/ps/glossary/.

V. POLICY

The Identification and Authentication policy seeks to control access among users, applications, and data. Controlled access means that systems require input of identifying information so that only authorized users and applications are granted access to a component of the infrastructure, a device or a service.

This policy ensures that the identification and authentication methodology applied will be commensurate with the type of access needed and the sensitivity of a system's data. This criteria is described in 08-04-NJOIT, *130-01 Asset Classification and Control Standard*. The business or department owners within the information area involved will make the decision about the levels and types of identification and authentication that will be deployed in accordance with state and/or federal laws, statutes, and regulations.

If strong identification and authorization mechanisms are used, the risk that unauthorized users will gain access to a system will be significantly decreased.

The following Identification and Authentication policies must be adhered to:

A. All users of the State of New Jersey information systems must be uniquely identified and authenticated before access is permitted to the system or application.

B. Multi-factor authentication is required for remote and/or privileged users.

C. Identification and authentication of users at the network level can be supplemented by identification and authentication at the application level to provide increased security.

D. Privileged users must not use their primary account (for email, Internet access and file shares) and will require a second user ID for privileged access to the system.

E. For system to system connections, systems must uniquely identify and authenticate before allowing a connection.

F. Management of identifiers and authenticators must be guided by State Policy.

G. Authenticator feedback must be obscured during authentication.

H. Cryptographic authentication must follow approved State of New Jersey Standards.

VI. RESPONSIBILITIES

A. Department and Agency

Departments and Agencies must ensure that a strong identification and authentication process is in place to protect the privacy of users by reducing the risk of unauthorized disclosures. This can only happen if access controls are appropriately designed based upon the sensitivity and criticality of the information and the risks associated with that information.

Departments and Agencies must determine if a user is authorized to access an IT system, and that distinct steps of identification and authentication are in place. Identification concerns the manner in which a user provides his unique identity to the IT system. The identity may be a name (e.g., first or last) or a number (e.g., account number). The identity must be unique so that the system can distinguish among different users.

B. System Administrators

System administrators must implement State of New Jersey Identification and Authentication Standards that manage and administer a system in a secure manner.

System administrators must ensure that accounts provide users with the lowest level of privilege needed to perform their tasks as requested by their managers.

System administrators must report all non-compliance to the proper authorities according to 11-02-NJOIT, *190 – Incident Management Policy*.

C. Chief Information Security Officer

The CISO must create, publish and communicate this policy to all personnel, and must ensure that this policy is reviewed at least annually and updated as required.

VII. EXCEPTIONS AND NON-COMPLIANCE

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

Failure to comply with this policy may result in disciplinary action. A compliance exception must be requested if there is an inability to comply with this policy because of a business reason or system constraint. Exceptions and non-compliance with this policy shall be managed in accordance with Policy 08-02-NJOIT, *111 – Information Security Managing Exceptions*.

Signature on File *10/27/2014*

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