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: 172 – Access Control Management Policy

NO:	SUPERSEDES:
14-29-NJOIT	N/A
LAST REVIEWED: November 13, 2014	**DATE PUBLISHED:** November 13, 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 policy is to specify how the Executive Branch of New Jersey State Government will control access to the State's information assets and resources. It is also to ensure the appropriate controls are in place for accessing State Government's information and facilities based on business needs and security requirements. These methods for authorizing access to the State's assets shall be in accordance with local, state, and federal security requirements and 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

This policy is designed to ensure that access controls protect all of the State's information resources within State or hosted provider facilities. Access to information and business processes should be controlled on the basis of business and security requirements.

This policy shall account for and reflect the State's guiding principles for information dissemination and authorization, and these principles shall be supported by formal standards and procedures and by clearly defined responsibilities. Access controls are both logical and physical and should be considered together. Below are industry standard polices to which State departments and agencies should adhere:

A. Least Privilege

Access control standards for State systems and facilities should grant each person with only the lowest level of access needed to accomplish assigned tasks.

B. Managing User Accounts

Access to all systems must be authorized by the department or agency of that system, and such access, including the appropriate access rights (or privileges), must be recorded in an Access Control List. These lists should reflect the level of confidentiality, sensitivity, privileges and value of the data. The data should be safeguarded accordingly and reviewed regularly by System Administrators.

User accounts will be modified for privileges, deactivated, or deleted by System Administrators when authorized by the system owner or a department or agency representative.

User accounts should be logged and audited periodically.

User accounts that are inactive for a period of 6 months will be automatically disabled or deleted.

C. Securing Unattended Workstation

Departments and agencies should ensure that all State and Contractor personnel can prevent access to their workstations while unattended by performing a session lock. A session lock should be performed automatically after a period of inactivity as determined by the System Administrator.

D. Managing Network and Operating System Access Controls

Only managers and administrators with proper authority and work-related need will be granted access to the controls for determining who has access to the network and operating systems. Managers and administrators with escalated privileges will require specific approval from senior management.

E. Warning Banner

A warning banner will be displayed before access to the resources on the State of New Jersey network is permitted. Users must acknowledge that they have seen the banner before being granted access, usually by clicking on an icon on the computer screen. The banner must explicitly state that user access of the State's network may be monitored and that the user may be subject to criminal and civil penalties if access is abused. The access controls will be addressed in accordance with 14-04-NJOIT, *1703 – Disclaimer Policy*.

F. Managing Passwords

Users must select passwords that meet the regulations and guidelines for optimal security safeguards provided by local, State and federal authorities. Passwords shall not be shared with any other person. The access controls will be addressed in accordance with 14-32-NJOIT, *177 – Password Management Policy*.

G. Controlling Remote User Access

Remote access control procedures must provide robust identification, two-factor authentication, and FIPS 140-2 approved encryption techniques. The access controls will be addressed in accordance with 11-01-NJOIT, *179 – Remote Access Policy*.

H. Physical Access Control

Physical access to restricted areas shall be controlled with strong identification and authentication methods. All electronic cabling and network infrastructure components shall be restricted to authorized personnel only. Visitor access will be logged, and all visitors visiting restricted areas such as data centers, computer rooms, communication closets and etc. will be escorted at all times.

I. Monitoring System Access and Use

Access to State networks and systems will be monitored and logged to identify potential misuse of systems and/or information.

J. Giving Access to Files and Documents

Access to information and documents must be carefully controlled, ensuring that only authorized personnel have access to sensitive information.

K. Managing Higher Risk System Access

Access controls for highly sensitive information or high-risk systems will be set in accordance with the value and classification of the information assets being protected. Sensitive, critical information should be isolated if necessary to safeguard it. Systems shall be classified according to the highest classification of any information stored on that system. The access controls will be addressed in accordance with 08-04-NJOIT, *130 – Information Asset Classification Control Policy*.

L. Granting Access To Third Parties

Access to systems, networks, information, and premises should only be granted to third parties in controlled circumstances and should be approved with clear reference to the reason why access is necessary. These reasons include approved on-site or remote maintenance or a need for support from specialists who will require access to systems and/or premises where systems are located. Both physical and logical access to diagnostic and configuration ports should be controlled. The access controls will be addressed in accordance with 09-11-NJOIT, *169 – Business Entity and/or IT Services Extranet Policy*.

M. Access Control Framework

Access control requirements should be documented. Access control rules and access rights for each user or group of users should be clearly stated in an accessible policy statement. Users and service providers should be given a clear statement of the business requirements to be met by access controls. The access controls will be addressed in accordance with 14-18-NJOIT, *174 – Network Security Policy*.

N. Controlled Pathway

The State will use controlled pathways to improve security for remote users and enforce secure information flow. Networks are intended to be shared by both local and remote users, and control over the routing used will enable the network administrator to ensure that the data is accessed through pre-agreed channels.

O. Wireless and Mobile Access

Agencies will protect their systems from the security risks of mobile and wireless computing by implementing strong security controls for encryption, user authentication, and end-point protection mechanisms. Anti-virus protection and perimeter controls shall be properly configured. The access controls will be addressed in accordance with 14-03-NJOIT, *173 - Wireless Network Security Policy* and 12-02-NJOIT, *132 – Portable Computing Use and Temporary Worksite Assignment Policy*.

P. Public Facing Websites

Any agency or department that deploys public facing websites should review content before posting onto the site to ensure that non-public state information is not contained on the site. Agencies should ensure the security of public web servers and supporting infrastructure by removing unnecessary services and patching and updating operating systems as they become available. Systems should be tested periodically using the State's Vulnerability Assessment program, for any potential vulnerability, in accordance with the 12-04-NJOIT, *184-Information Security Vulnerability Management Policy*.

VI. RESPONSIBILITIES

A. Departments and Agencies

IT Directors must establish, document, and review access control policies, standards, and procedures based on business and security requirements for access.

VII. 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 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 — *11/13/2014*

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