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 165 – Firewall Management Policy	**POLICY NO:** 15-03-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 01/22/2015
	VERSION: 1.0	**LAST REVIEWED:** 01/22/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to define requirements for managing electronic firewalls that protect the State of New Jersey's systems and infrastructure. This policy is designed to assist IT administrators in establishing strict rules for firewall configuration and management. It aims to minimize the risk of unauthorized access to networks, loss of sensitive or confidential information, and/or damage to the State of New Jersey's critical internal systems and information technology assets.

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 all State of New Jersey Departments, Agencies, State Authorities, "in but not of" entities, their employees, contractors, consultants, temporary employees, and other workers including all personnel who are tasked with the protection of the State of New Jersey resources, systems, and infrastructure.

4 DEFINITIONS

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

5 POLICY

The following requirements provide a policy for managing a firewall connected to the State of New Jersey's networks:

5.1.1 A baseline firewall configuration shall be created for each firewall. Changes to the firewall device's hardware, software, or operating environment as well as any modification to the rule base shall be documented in accordance with 14-09-NJOIT *168 – Change Management Policy*. Firewall configuration changes shall be backed up and secure copies maintained.

5.1.2 Firewall rule submissions and configuration changes are to be scheduled. The OIT schedule for submission is 3 p.m. on Friday and, for configuration changes, the following Wednesday.

5.1.3 Emergency firewall rules must be approved by the Deputy CTO for OIT's Infrastructure Support Services and the Manager for OIT's Statewide Office of Information Security (SOIS).

5.1.4 Agencies are to identify personnel who are authorized to submit firewall rules on the agency's behalf and provide a list to the manager of OIT's SOIS.

5.1.5 Firewall rules are to be reviewed yearly and removed if no longer required.

5.1.6 All State firewalls shall be configured to "deny by default" and block all traffic that has not been expressly permitted by firewall policy.

5.1.7 All State firewall policies should be based on source and destination as well as content and sensitivity of the traffic. A standard configuration will be developed and implemented under the direction of the State's Information Security Officer.

5.1.8 Traffic inbound to the State's networks containing ICMP (Internet Control Message Protocol) traffic will be blocked at the perimeter.

5.1.9 IPsec or SSL Virtual Private Networks (VPN's) should be used to authenticate users by firewalls utilizing an identity policy.

5.1.10 An explanation of each rule should be included with its rule base entry.

5.1.11 Firewalls should have an inactivity network disconnect associated with its firewall policy and that time period of inactivity is up to the discretion of the agency and the application requirements. Firewall default is set to 60 seconds.

5.1.12 Management logging and auditing shall be implemented on all firewall devices that support logging and auditing. Log events must be forwarded to the State's Security Incident Event Management (SIEM) system. Firewalls must utilize an authentication mechanism (i.e. AAA authentication, TACACS, Radius Authentication) that provides accountability for the user and accessibility through a secure channel (i.e. SSH).

5.1.13 All firewalls should record their traffic, especially blocked traffic, and this data should be reviewed regularly.

5.1.14 All State firewalls shall be physically secured by being installed in an access-controlled area. Access to the firewalls shall be limited to the appropriate Agency Wide Area Network (WAN) security administrators.

5.1.15 All Agencies shall utilize dedicated hardware devices for firewall protection to ensure that all confidential, proprietary and/or sensitive information is secure within the state's networks. Firewalls shall conform to the ICSA Labs compliance criteria, Version 4.0 or the latest version.

6 ROLES AND RESPONSIBILITIES

The State of New Jersey

6.1.1 The Wide Area Network Unit within the Office of Information Technology will configure and manage the State's firewalls in accordance with best practices and industry standards in order to protect the state's networks. Department and Agency staff members are responsible for the management of agency firewalls, unless an agreement has been made with OIT's WAN unit for management of said device(s). Any Departments, Agencies, State Authorities, "in but not of" entities, requiring deviations from the standard configuration must formally request these changes and take responsibility to provide compensating controls to ensure the security of the state's networks.

6.1.2 The Statewide Information Security Office within the Office of Information Technology will set up and manage the authentication of firewalls and perform the administrative functions in order to maintain the lifecycle management processes in accordance with best practices and industry standards.

6.1.3 The Statewide Cyber Security Threat Mitigation Committee (CSTMC) will approve, publish, and update the security standards under the guidance of the State's Information Security Officer.

7 ENFORCEMENT

Any firewall Authorized User found to have violated this policy may be subject to disciplinary action by the appropriate department or agency, and loss of firewall management privileges. **IN ADDITION, VIOLATORS MAY BE SUBJECT TO CRIMINAL PROSECUTION, CIVIL LIABILITY, OR BOTH FOR UNLAWFUL USE OF ANY ACCESS.**

8 EXCEPTIONS AND NON-COMPLIANCE

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

Requests for exceptions for non-compliance with this policy shall be processed in accordance with Statewide IT Circular 08-02-NJOIT, *111 – Information Security Managing Exceptions.*