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 169 – Business Entity, IT Services and/or Extranet Policy	**POLICY NO:** 09-11-NJOIT	
	SUPERSEDES: NEW	**EFFECTIVE DATE:** 06/06/2009
	VERSION: 2.0	**LAST REVIEWED:** 01/22/2015

ATTN: Directors of Administration and Agency IT Managers

1 PURPOSE

The purpose of this policy is to provide the security controls and process for sponsoring Agencies and Business Entities when Information Technology (IT) services are planned for installation or made available to agencies and/or an extranet connection(s) to the State of New Jersey Next Generation Services Network (NGSN) is established or operating for the conduct of electronic business with the State of New Jersey.

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 personnel including, business entities, employees, temporary workers, volunteers, contractors and those employed by contracting entities, and others who are authorized to access enterprise information resources and/or systems regardless of the technology used for the connection.

4 DEFINITIONS

Please refer to the statewide policy glossary at http://www.state.nj.us/it/ps/glossary/index.html.

5 POLICY

All Sponsoring Agencies and their Business Entities utilizing IT and/or extranet services shall adhere to the following:

5.1.1 Business Entity service and/or extranet use are permitted only for legitimate State of New Jersey business purposes.

5.1.2 Sponsoring Agencies and Business Entities using extranet connections must employ best practices and make all reasonable efforts to protect the confidentiality, integrity, and availability of State networks, systems, and information. All computers connected to State internal networks via extranet technology must have up-to-date operating systems patches as well as up-to-date security software. Sponsoring Agencies are free to request verification of compliance from their Business Entity on a regularly scheduled basis. All connectivity established must be based on the least-access principle, where users are only given the access and privileges they need to complete their role, in accordance with the approved business requirements and the security review.

5.1.3 Changes cannot be made to an IT service or the extranet connection once approved without prior review and approval. Changes or enhancements to the IT service and/or extranet connection must be submitted through the System Architecture Review process as part of the Office of Information Technology's Change Management Control procedures.

5.1.4 The Office of Information Technology's Wide Area Network (WAN) personnel, Statewide Office of Information Security (SOIS) groups, the Business Entity, and the entity's Sponsoring Agency will collaborate on developing procedures that will define specific tasks, deliverables, roles and responsibilities for implementing and supporting each individual IT service and/or extranet connection.

5.1.5 Any cost incurred by a Business Entity for use of IT services and/or extranet connections is the responsibility of the Business Entity.

I. Departments and agencies must develop specific internal requirements and implementation practices that all contracted and/or sub-contracted entities must adhere to when accessing state information resources. Each department or agency must include at a minimum the following requirements and/or practices:

5.1.5.1 *Departments and agencies must ensure that all Contractor access is restricted to only that information needed to fulfill business contracts according to the least-access principle.*

5.1.5.2 *All contracts with external suppliers of services to departments and agencies must be monitored and reviewed in an appropriate manner by specific personnel with the authority and ability to review such contracts to ensure that information security requirements are being satisfied. Contracts must also include appropriate provisions to ensure the continued security of information and systems in the event that a contract is terminated or transferred to another supplier. All contracted and sub-contracted entities must be able to demonstrate compliance with the State's Information Security policies, standards and/or procedures.*

5.1.6 Departments and agencies must be cognizant of the information that is created, handled, stored, or copied as part of the contract agreement. Based on the value established through the asset classification process, the department or agency must take appropriate steps to track the usage of the information asset through the life cycle of the contract. The departments and agencies will assess the risk to information assets based upon the confidentiality, sensitivity or value of the information being disclosed or made accessible.

5.1.7 Departments and agencies must ensure that contractors provide written documentation specifying how information will be handled, stored, copied and/or protected. Departments and agencies will also ensure that contracted and sub-contracted entities have access only to information allowed under the contract. These requirements should be included in all agreements between the State and the Contracted Entity.

5.1.8 All departments and agencies must provide a non-disclosure agreement to all Contracted and Sub-Contracted entities.

5.1.9 All departments and agencies must ensure that all contracted and sub-contracted personnel working in State facilities are issued ID badges. Badges must be displayed at all times when personnel are working or visiting on State premises. The department or agency must collect badges upon termination or completion of a contract. State equipment and supplies must be returned. Departments and agencies will eliminate all contract personnel's access to facilities and remove any authentication and all means of access to systems after the contract has been completed or terminated. If applicable, departments and agencies will ensure that incoming e-mail to outside

personnel received on State systems is re-routed to an appropriate person once a contract ends.

5.1.10 Contracted and sub-contracted employees must be advised to report all on-site security incidences to the appropriate Department or Agency personnel.

5.1.11 The department or agency must ensure that personnel working for contracted and sub-contracted entities follow all applicable change control procedures and processes when testing or deploying data or systems and when connecting third-party owned equipment to the infrastructure while establishing outbound connections.

5.1.12 All contracted employees are required to comply with any and all mandated auditing regulations and/or requirements.

5.1.13 Privilege Escalation procedures must be followed when allowing contracted or sub-contracted entities access to any State systems.

5.1.14 Any computer/laptop/net book that is temporarily (less than five business days) connected to the Garden State Network must have up-to-date anti-malware protection and patches, and the department or agency must verify this state of readiness. For contracted work of durations longer than five business days, department or agency equipment must be used.

5.1.15 All software used by contracted or sub-contracted entities must be properly inventoried and licensed. Departments and agencies must obtain a written statement from the contractor that any software created and/or installed by the third-party is properly licensed and free of viruses and any other malicious code.

5.1.16 All third-party-owned maintenance equipment on the Garden State Network that is capable of connecting to the outside world via telephone lines, leased lines, wireless connectivity, or the Internet must remain disabled except when in use for authorized maintenance.

5.1.17 Upon completion or termination of a contract, the department or agency will ensure that all classified information is collected and returned or destroyed as applicable depending on the media upon which that information resides.. If information is destroyed, the third party will provide an auditable certification of that destruction according to the NIST Special Publication 800-88 Guidelines for Media Sanitization.

6 NON-COMPLIANCE

Any State of New Jersey personnel found to have violated this policy may be subject to disciplinary action, up to and including termination of employment by the applicable department or agency. Any business entity found in violation of this policy may result in a filtered connection or be denied future IT services and/or extranet access.