# Business Entity, IT Services and/or Extranet Policy and Procedure

**STATEWIDE POLICY NUMBER: 09-11-NJOIT**

Approved By: Christopher J. Rein, Chief Technology Officer

Version: 2.0
Effective: 07/06/2009
Revised: 01/22/2021
Supersedes: *09-11-P1-NJOIT; Appendix A; Appendix B*

## PURPOSE

This Policy and Procedure establish the security controls and requirements for Sponsoring Agencies and Business Entities when an Information Technology (IT) service or an extranet connection to the Garden State Network (GSN) is required to conduct business with the State of New Jersey.

## SCOPE

All Executive Branch departments and State agencies (Agencies) are directed to cooperate fully with the New Jersey Office of Information Technology (NJOIT) and the Chief Technology Officer (CTO) to implement the provisions of the Policy and Procedure, and to ensure effective use of information technology.

This Policy and Procedure apply to all business entities, their employees, contractors, and those employed by contracting entities, and others who are authorized to access State enterprise information resources and/or systems, regardless of the technology used for the connection.

## POLICY

NJOIT and the CTO require compliance with the *Statewide Information Security Manual* (SISM), *Third Party Management Policy (TP)* established March 2018 by the New Jersey Office of Homeland Security and Preparedness.

**REQUIREMENTS**

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

- Business Entity IT service and/or extranet use is permitted only for legitimate State of New Jersey business purposes.

- 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 authorized to request verification of compliance from their Business Entity quarterly. All connectivity established must be based on the "least-access principle", where users are granted only the access and privileges necessary to complete their role, in accordance with the approved business requirements.

- Changes or enhancements to the IT service and/or extranet connection must be submitted through the NJOIT Information Security Unit (ISU). Changes cannot be made to an IT service or the extranet connection, once approved, without prior review and approval by the ISU.

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

- 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. All Agencies must include, at a minimum, the following requirements and/or practices:

    - Agencies must ensure that all Business Entity or contracting agency access is restricted to only that information needed to fulfill business contracts according to the least-access principle.

    - All contracts with external suppliers of IT services to Agencies must be monitored and reviewed in an appropriate manner in accordance with the *SISM, Third Party Management Policy, Contract Requirements (TP-03)*. Specific personnel with the authority and ability to review such contracts are to ensure that information security requirements are being satisfied. Contracts must also include appropriate provisions to ensure the continued security of information and systems if a contract is terminated or transferred to another supplier. All contracted and sub-

contracted entities must be able to demonstrate compliance with the *SISM*.

- Agencies must be cognizant of the information assets that are created, handled, stored, or copied as part of the contractual agreement. Based on the classification of the assets, the Agency must take appropriate steps to track the usage of information assets through the life cycle of the contract. Agencies will assess the risk to information assets based upon the confidentiality, sensitivity or value of the information being disclosed or made accessible. Agencies must be able to demonstrate compliance with the data classification policies set forth by the *SISM (Reference SISM," Security Categorization Policy (SC)" and "Appendix A-Security Categorization Considerations" for more information)*.

- Agencies must ensure that contractors provide written documentation specifying how information will be handled, stored, copied and/or protected during the contracting period and then once accepted, this written documentation will become part of the contract. Agencies will also ensure that contracted and sub-contracted entities have access only to information assets as specified in the contract. These requirements should be included in all agreements between the State and the contracted Business Entity.

- All contracted and subcontracted business entities will be expected to abide by the confidentiality requirements set forth in the Terms and Conditions of the agreement they have executed with the State of New Jersey. The State of New Jersey reserves the right to request the execution of a non-disclosure agreement (NDA) in its sole discretion.

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

- The 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 State of New Jersey infrastructure while establishing outbound connections. Agencies must be able to demonstrate compliance with the *SISM, Change Management Policy (CH).*

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

- Privilege escalation procedures must be followed when allowing contracted or sub-contracted entities access to any State systems. Agencies must be able to demonstrate compliance with the SISM,

*Access Management Policy (AC)* and 179-01-P1-NJOIT, *Remote Access Procedure*. To obtain a copy of 179-01-P1-NJOIT, *Remote Access Procedure*, contact the NJOIT ISU.

- All software used by contracted or sub-contracted entities must be properly inventoried and licensed. 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.

- All third party-owned maintenance equipment on the Garden State Network connected either by telephone lines, leased lines, through wireless connectivity, or the internet must remain disabled, except when in use for authorized maintenance.

- Upon completion or termination of a contract, the Agency will ensure that all data is either collected and returned or destroyed as applicable, depending on the media upon which that information resides, in compliance with State records management policies. 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.

**PROCEDURES**

All Sponsoring Agencies and their Business Entities utilizing an IT service, or an extranet connection must adhere to the following:

- The Sponsoring Agency and the Business Entity and if applicable, NJOIT, must complete the *Extranet Connection Form* (OIT-0145).

- The Sponsoring Agency must maintain all documentation associated with extranet activity. It must review the details of the documentation annually to ensure the accuracy of the content. The Sponsoring Agency must also notify all parties if any contact information changes.

- Any Agency that wishes to connect to a pre-existing IT service and/or extranet connection must execute their own *Extranet Connection Form* and return it to the ISU.

- When access is no longer required, the Sponsoring Agency must notify NJOIT's ISU within thirty (30) business days. The ISU will then terminate connectivity.

## Establishing Connectivity

The Sponsoring Agency will work with the Business Entity to establish the IT service and/or extranet connectivity. Prior to establishing connectivity, the Sponsoring Agency and Business Entity will complete the *Extranet Connection Form* and submit copies to the NJOIT ISU at the email address provided on the *Extranet Connection Form*. The ISU will coordinate with the necessary NJOIT groups to build the connection.

## Making Changes to Existing Business Entity IT Services or Extranet Connections

- All Business Entity IT services or Extranet changes and modifications must be submitted by the Sponsoring Agency to the NJOIT ISU.
- An updated *Extranet Connection Form* is required, and notification must be sent and reviewed by the NJOIT ISU before changes or modifications are implemented. All access must be listed on the form. Highlight any changes to be made.

## Access Maintenance and Termination

- The NJOIT ISU, Business Entity, and Sponsoring Agency will collaborate on developing IT Service or Extranet-specific contingency procedures to follow in the event of an outage or service disruption that affects business processes. It is the responsibility of the Sponsoring Agency to ensure these collaborative efforts are developed. Such a procedure will define roles and responsibilities including, but not limited to the following:
    - Maintaining active IT services/extranet equipment and data circuits;
    - Tracking and monitoring equipment;
    - Using an approved notification process;
    - Specifying points of contact for all stakeholders;
    - Defining access to equipment; and
    - Setting the process for resolution and recovery.
- The NJOIT ISU group will conduct a periodic review, annually at minimum, of all existing IT services and extranet connections, to ensure that all existing connections are actively in use, still needed, and are configured properly for current needs.

- Unused connections will be terminated with at least fourteen (14) days prior notice provided to the Sponsoring Agency.
- The Sponsoring Agency will be responsible for retrieving any State-owned equipment from the Business Entity.
- Should a security incident necessitate a change to existing permissions, or the termination of connectivity, the NJOIT ISU group will notify the Sponsoring Agency of the change prior to taking any action; however, the ISU reserves the right to terminate connectivity in the event of an emergency.

## RELATED DOCUMENTS AND FORMS

*Statewide Information Security Manual* – To obtain a copy, please contact your Agency's Chief Information Officer.

179-01-P1-NJOIT, *Remote Access Procedure* – To obtain a copy, please contact the NJOIT ISU.

*Extranet Connection Form* (OIT-0145)

## COMPLIANCE AND ENFORCEMENT

Exceptions
All requests for compliance exceptions must be based on a valid restriction that prevents full compliance with the policy, standard or procedure. Exception requests must be approved by the Agency CIO or CISO and forwarded to the New Jersey Cybersecurity and Communications Integration Cell (NJCCIC) and the New Jersey Office of Information Technology (NJOIT) for acceptance and cataloging.

Non-compliance
Any State of New Jersey personnel found to have violated this Policy and/or Procedure may be subject to disciplinary action, up to and including termination of employment by the applicable department or agency. Any Business Entity personnel found in violation of this Policy may result in a filtered connection or be denied contracts for future IT services and/or extranet access. Contract requirements are defined in *SISM, Third Party Management Policy (TP).*

## AUTHORITY

N.J.S.A. C.52:18A-224 et seq., known as "The Office of Information Technology Reorganization Act."

## ADMINISTRATION

This Policy must be reviewed annually; however, the CTO reserves the right to change or amend it at any time to comply with changes in agency procedures.

Any changes or amendments will be announced and made available on NJOIT's website.

Changes in this Policy will be effective upon such publication, distribution, or as defined in the policy statement.

This Policy is administered and monitored by the CTO at 300 Riverview Plaza, Trenton, NJ 08625.

***SIGNATURE ON FILE***
CHRISTOPHER J. REIN, CHIEF TECHNOLOGY OFFICER

**01/22/2021**
DATE

## DOCUMENT HISTORY

| Version | Description of Modification | Publication Date |
|---|---|---|
| 1.0 | Original Published Date | 07/06/2009 |
| 2.0 | Annual Review/*09-11-P1-NJOIT; Appendix A; and Appendix B* are no longer in use. | 01/22/2021 |

*Printed copies of this document are uncontrolled; please refer to the NJOIT website for the current version in effect. Please visit our website at: tech.nj.gov*

## CONTACT

NJOIT Information Security Unit (ISU) at *OIT.vpnadmin@tech.nj.gov*