State of New Jersey
Office of Information Technology

File Transfer Guide

TASKS AND DELIVERABLES

Assessments/Plans

The Contractor shall provide a detailed system design document showing Security Plan. Logical and physical diagrams are required.

- **Security Plan**

  The Contractor must provide a security plan for the proposed solution. The document shall describe the administrative, physical, technical and systems controls to be used by the system and/or services. The Contractor's security plan must, at a minimum, provide security measures for the following areas:

  - Facilities Physical Security and Environmental Protection
  - System Security
  - System Data Security
  - Network Security
  - Administrative and Personnel Security

  The security plan shall provide for review of the Contractor's operations and control system for the proposed solution. The Contractor shall have the capability to detect and report attempted unauthorized entries into the facility and system. All security requirements for the Contractor apply to development, testing, production and backup systems.

  In addition, the security plan the Contractor shall identify, address and/or define:

  - Regulations and security requirements – how the Contractor will address security requirements such as PCI, HIPAA, FISMA and etc.
  - System, Administrative and Personnel Security - the security responsibilities of and supervision required for information owned and / or operated by the Contractor. Security responsibilities include responsibilities for administration of the infrastructure, implementing or maintaining security and the protection of the confidentiality, integrity, and availability of information systems or processes.
  - Workforce Security - the control process for hiring and terminating of Contractor's employees, and method used for granting and denying access to the Contractor's network, systems and applications. Identify and define audit controls when employment of the employee terminates. Identify rules of behavior.
  - Role-based security access – the products and methods provides role-based security, access enforcement and least privilege.

- Account Management – the products and methods identify and control the account types to meet defined regulation and security requirements.
- Password Management – the appropriate password management controls to meet defined regulation or security requirements.
- Logging / Auditing controls – the Contractor's audit control methods and requirements. The controls must address but not limited to all user access and user identification linked to any changes to the system and data, and provide an audit process that will make all audit data accessible to state and federal audit staff. The audit trail of all transactions should track date, time, user, and end-user device that initiated the transaction. The audit data must be protected, non-repudiated and restricted to authorized staff. Retention of the audit records will be retained online for at least ninety days and further preserve offline for a period of the contract or required State and Federal laws and regulations.
- Incident Management – the methods for detecting, reporting and responding to an incident, vulnerabilities and threats. The methods are tested and exercised.
- Vulnerability / Security Assessment – the products and methods used for scanning for vulnerabilities and remediation of the vulnerabilities. Identify and define methods used for initiating and completing security assessments. All systems and applications shall be subject to vulnerability assessment scans by an independent and accredited third party on an annual basis.
- Application Security – where the Contractor is providing application hosting or development services, the Contractor at a minimum shall run application vulnerability assessment scans during development and system testing. Vulnerabilities shall be remediated prior to production release.
- Application and Tenant Isolation – where the Contractor is providing application hosting and/or development services, the Contractor will isolate the computing environment (compute/partition, network and storage/media.)
- Anti-virus / malware controls – the products and methods for anti-virus and malware controls that meet industry standards. It shall include policy statements that require periodic anti-viral software checks of the system to preclude infections and set forth its commitment to periodically upgrade its capability to maintain maximum effectiveness against new strains of software viruses.
- Network Security – where the Contractor has access to State confidential data, and that data will traverse the Contractor's network, the Contractor shall maintain the Contractor's network security to include, but not be limited to: network firewall provisioning, intrusion detection and prevention, denial of service protection, annual independent and accredited third party penetration testing, and maintain a hardware inventory including name and network address. The Contractor shall maintain network security that conforms to current standards set forth and maintained by the National Institute of Standards and Technology (NIST), including those at: **http://web.nvd.nist.gov/view/ncp/repository**.
- Database – the products and methods for safeguarding the database(s).

- Data Integrity – the products and methods on the integrity of all stored data and the electronic images, and the security of all files from unauthorized access. The Contractor must be able to provide reports on an as-needed basis on the access or change for any file within the system.
- Server and infrastructure – the products and methods for "hardening" of the hardware' operating systems and software.
- Wireless, Remote and Mobile Access – where the Contractor has access to State confidential data, and that data traverses the Contractor's network, the Contractor shall have security controls for provisioning accounts, authorization, account/credential verification, audit/logging, VPN, and TCP/UDP ports restrictions.
- Transmission - the products and methods on how its system addresses security measures regarding communication transmission, access and message validation.
- Continuous Monitoring – where the Contractor has access to State confidential data, and that data will traverse the Contractor's network, the Contractor shall have products and methods for monitoring malicious activity, malware, intrusions and audit records within the Contractor's network.
- Security Audit – the Contractor must allow State assigned staff full access to all non-secure operations for security inspections and audits which may include reviews of all issues addressed in description of the security approach and willingness to enter into good faith discussions to implement any changes.
- Change / Configuration Management and Security Authorization – the Contractor has established a change / configuration methodology, establish a baseline configuration and track changes to the configuration. Identify and maintain a list of software programs authorized to execute on a system. When the Contractor has a major change to the system or application, the State's project manager is notified and a security reauthorization must be approved.
- Risk Management – the Contractor has established a risk management plan, technical and security risks are identified, reported and mitigated.

Extranet Plan

Extranet Use Cases

- The need arises that an external 3rd party needs to initiate file transfers to a GSN Department or Agency.
- Information Exchange between external parties needs to be secured or routed over a private connection.
- Vendors, 3rd Parties or other External parties want to build a private connection to an entity on the GSN, while avoiding the uncertainty of using the Internet as a medium. Utilizing the GSN Extranet service via private line allows bandwidth to be guaranteed and eliminates the fluctuations of speed and latency that would otherwise be impacted on the Internet.

Extranet Options

The communication links between the State of New Jersey and the contractor can be through a dedicated circuit or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints.

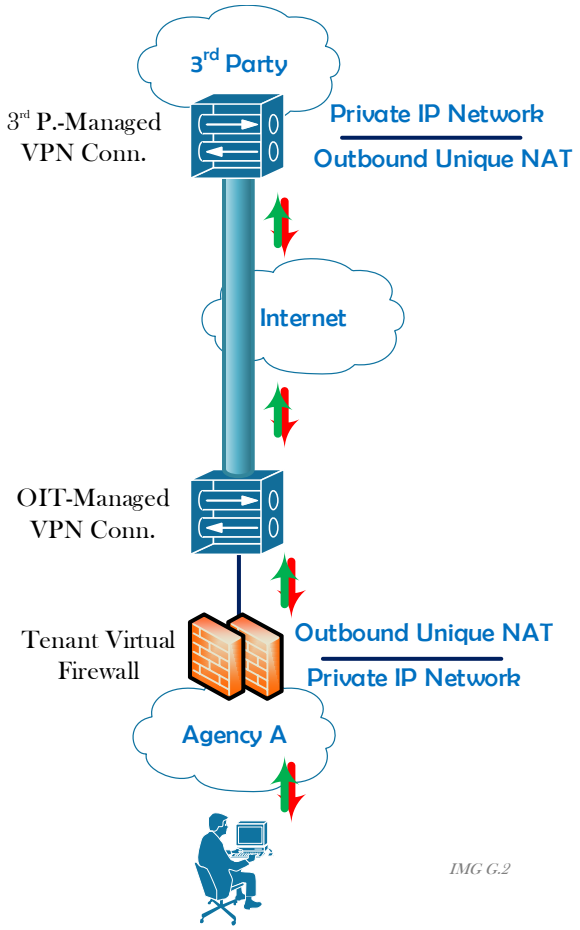
The contractor must work with the sponsoring agency and OIT to establish an Extranet Partner relationship. The State of New Jersey and the Contractor will be required to follow the State's Extranet Policy and Procedure, and complete the application form, MOU, operational form and security controls assessment checklist.

The State agency and external 3rd Party must agree on the Extranet service level they will be utilizing for the connection, the cost of the connection and who will be paying for the agreed upon services.

The State currently supports the following four service levels:

- Extranet Bronze – Single IPSEC Tunnel over the Internet.
- Extranet Silver – Single dedicated circuit from a telecommunications carrier.
- Extranet Gold – Dual IPSEC Tunnel over the Internet from our HUB and Hamilton Data Centers.
- Extranet Platinum – Dual dedicated circuits from a telecommunications carrier from our HUB and Hamilton Data Centers.

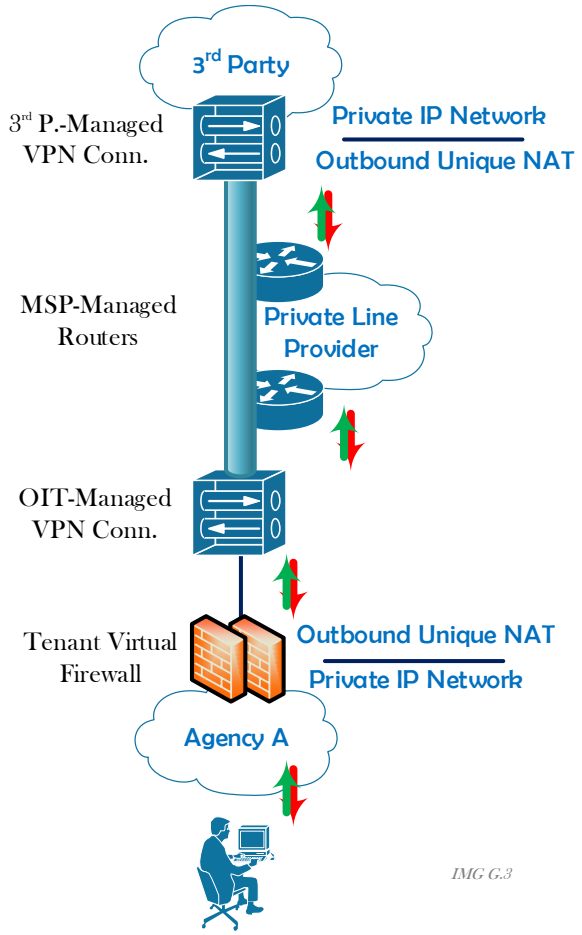
Extranet Topology and Technologies



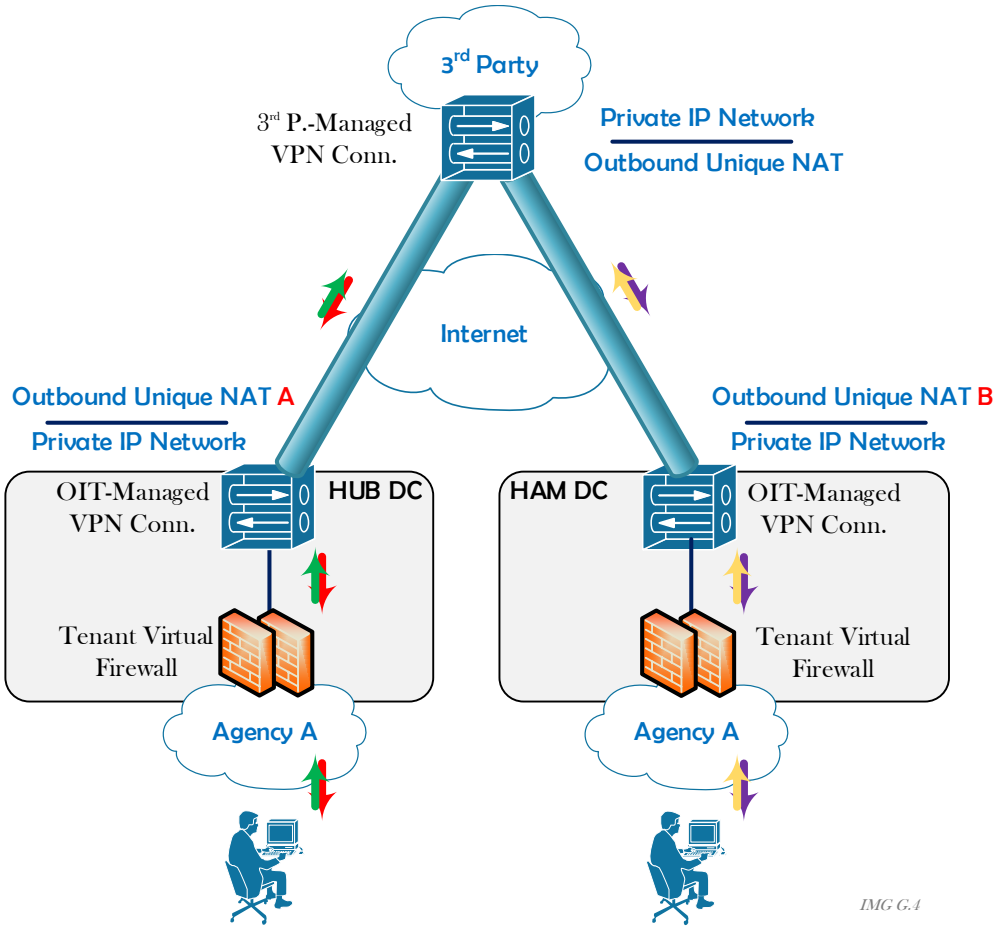
Extranet Specifics and Topology (Bronze)

- Various IPSec configuration parameters are supported and should at a minimum meet the recommended values as defined by NJOIT's GSN Technical Architects.
- Bandwidth over the Internet is not guaranteed.
- Internet instability may cause disruption of this tunnel, therefore this Extranet model is considered best effort.

Extranet Specifics and Topology (Silver)

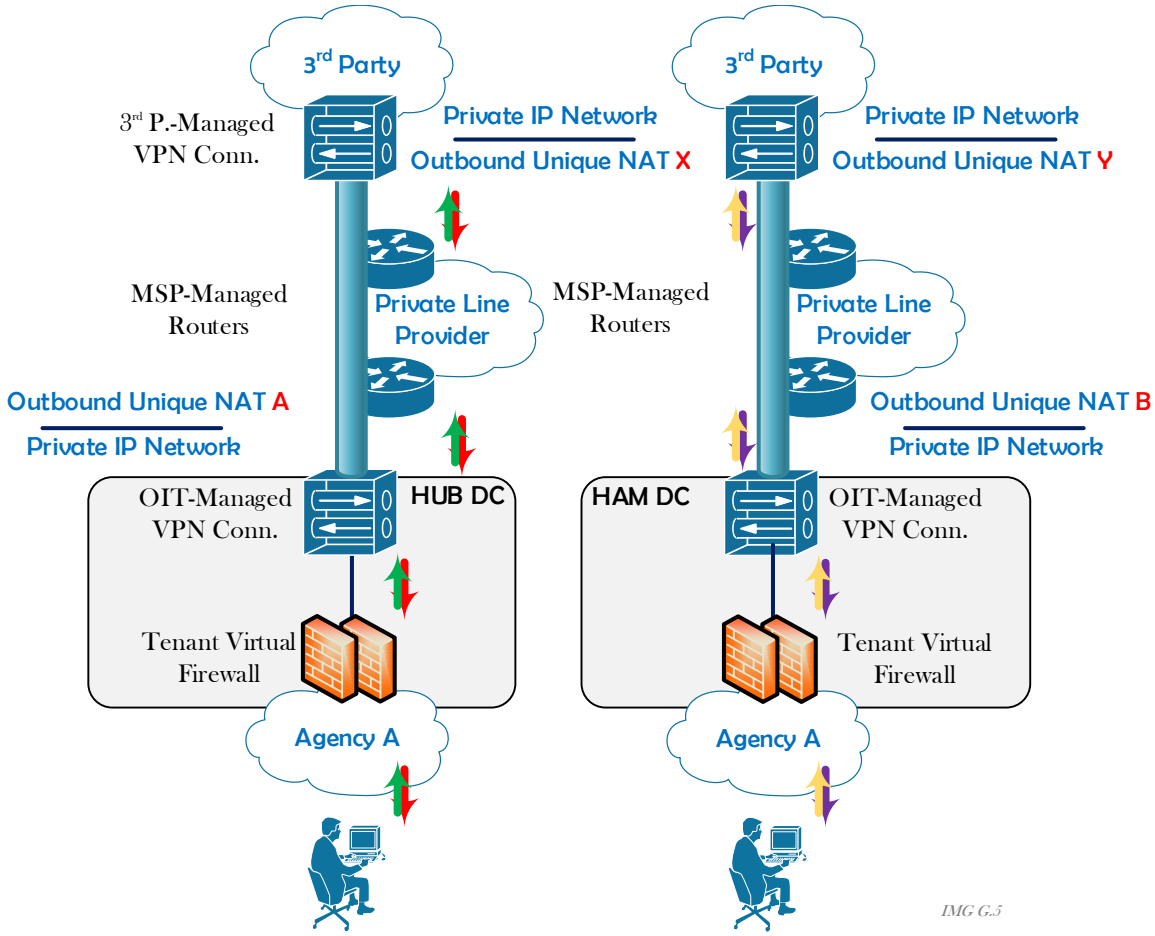


- All management and administration of the physical connectivity to the 3rd party carrier router is handled by the OIT Data Center Infrastructure Group and all equipment meet the Data Center's Electrical standards. (The Carrier Router and circuit must terminate at the West Trenton or Hamilton Data Centers.)
- Management of the Private Line Provider is the responsibility of the vendor or the Agency requesting service.
- Bandwidth over Private Circuits is typically guaranteed (depending on what the 3rd Party Vendor has requested from the Carrier)
- Incidents determined to be fault of the 3rd Party or Private Line Provider are the responsibility of the Agency or 3rd Party to remediate.



Extranet Specifics and Topology (Gold)

- Similar attributes and requirements to the Extranet Bronze Service, only dual-homed
- Each Data Center connection acts independently, and provides Unique NAT addresses at each connection point
- Applications can be configured to use one or both paths (depending upon the configuration of the App and the DNS resolution of IP Addresses for each tunnel.
- Traffic across each tunnel for similar IP Advertisements are treated as Active/Standby to avoid asymmetric traffic flow (traffic cannot leave through one VPN and return through the other – this traffic will be dropped).



Extranet Specifics and Topology (Platinum)

- Similar attributes and requirements to the Extranet Silver Services, only dual-homed with dual private carriers
- Each Data Center connection acts independently, and provides Unique NAT addresses at each connection point
- Applications can be configured to use one or both paths (depending upon the configuration of the App and the DNS resolution of IP Addresses for each tunnel.
- Traffic across each tunnel for similar IP Advertisements are treated as Active/Standby to avoid asymmetric traffic flow (traffic cannot leave through one VPN and return through the other – this traffic will be dropped).

Transmission of Files

The State of New Jersey supports multiple methods for data transfers internally within the Garden State Network or external to an extranet or business partner. The transmission of all files between the contractor and the State system must be transferred securely using the State file transfer methodology. The State will work with the contractor in the implementation of the file transfer process. The secure file transfer must meet the state and federal security guidelines and standards.

The State of New Jersey provides both asynchronous and synchronous file transfer methodologies.

Synchronous:

1) Connect:Direct Secure+ is a supported option for file exchange with the State of New Jersey IBM mainframe.

2) FTPS over SSL (Explicit – port 21) is a supported option for file exchange for connections originating from the State of New Jersey IBM Mainframe. Must support RFC2228.

3) SFTP (FTP over SSHv2 or greater) is a supported option for file exchange with State of New Jersey distributed servers and IBM Mainframe.

Asynchronous:

1) The State of New Jersey's Managed File Transfer (MFT) is a supported option for non-automated or "ad-hoc" file exchange with State of New Jersey. A client license is required.

2) The State of New Jersey's Managed File Transfer-DataBridge (MFT Databridge) is a supported option for automated file exchange with the State of New Jersey.

The contractor will be required to test the file transfer with the State system on all file transfers prior to full implementation.

During the life of the contract, the State may revise or change the file transfer method and/or format for the transmission of files to accommodate real time processing, and use case specific information and the contractor shall be required to conform to all requirements.

Reference:

NIST Special Publication 800-47 - Security Guide for Interconnecting Information Technology Systems (http://csrc.nist.gov/publications/nistpubs/800-47/sp800-47.pdf)

Data Confidentiality

All non-public financial, statistical, personnel, customer and/or technical data that is supplied by the State to the Contractor, or that the Contractor obtains through its work for the State are confidential. The Contractor must secure all data from manipulation, sabotage, theft or breach of confidentiality. The Contractor is prohibited from releasing any financial, statistical, personnel, customer and/or technical data obtained from the State that is deemed confidential. Any non-Contractual use, sale, or offering of this data in any form by the Contractor, or any individual or entity in the Contractor's charge or employ, will be considered a violation of this Contract and may result in Contract termination and the Contractor's suspension or debarment from State contracting. In addition, such conduct may be reported to the State Attorney General for possible criminal prosecution.

The Contractor shall assume total financial liability incurred by the Contractor associated with any breach of confidentiality subject to the liability provisions of this RFP.

The Contractor will not access the State of New Jersey's User Accounts or data, except (i) in the course of data center operations, (ii) response to service or technical issues or (iii) at State of New Jersey's written request.

CONTRACTOR'S CONFIDENTIAL INFORMATION

a) The obligations of the State under this provision are subject to the New Jersey Open Public Records Act ("OPRA"), N.J.S.A. 47:1A-1 et seq., the New Jersey common law right to know, and any other lawful document request or subpoena.

b) By virtue of this contract, the parties may have access to information that is confidential to one another. The parties agree to disclose to each other only information that is required for the performance of their obligations under this contract. Contractor's Confidential Information, to the extent not expressly prohibited by law, shall consist of all information clearly identified as confidential at the time of disclosure and anything identified in Contractor's quotation as Background IP ("Contractor Confidential Information"). Notwithstanding the previous sentence, the terms and pricing of this contract are subject to disclosure under OPRA, the common law right to know, and any other lawful document request or subpoena.

c) A party's Confidential Information shall not include information that: (a) is or becomes a part of the public domain through no act or omission of the other party; (b) was in the other party's lawful possession prior to the disclosure and had not been obtained by the other party either directly or indirectly from the disclosing party; (c) is lawfully disclosed to the other party by a third party without restriction on the disclosure; or (d) is independently developed by the other party.

d) The State agrees to hold Contractor's Confidential Information in confidence, using at least the same degree of care used to protect its own Confidential Information.

e) In the event that the State receives a request for Contractor Confidential Information related to this contract pursuant to a court order, subpoena, or other operation of law, the State agrees, if permitted by law, to provide Contractor with as much notice, in writing, as is reasonably practicable and the State's intended response to such order of law. Contractor shall take any action it deems appropriate to protect its documents and/or information.

f) In addition, in the event Contractor receives a request for State Confidential Information pursuant to a court order, subpoena, or other operation of law, Contractor shall, if permitted by law, provide the State with as much notice, in writing, as is reasonably practicable and Contractor's intended response to such order of law. The State shall take any action it deems appropriate to protect its documents and/or information.

g) Notwithstanding the requirements of nondisclosure described in these Sections *Data Confidentiality* and *CONTRACTOR'S CONFIDENTIAL INFORMATION*, either party may release the other party's Confidential Information (i) if directed to do so by a court or arbitrator of competent jurisdiction, (ii) pursuant to a lawfully issued subpoena or other lawful document request, (iii) in the case of the State, if the State determines the documents or information are subject to disclosure and Contractor does not exercise its rights as described in Section *CONTRACTOR'S CONFIDENTIAL INFORMATION*(e), or if Contractor is unsuccessful in defending its rights as described in Section *CONTRACTOR'S CONFIDENTIAL INFORMATION*(e), or (iv) in the case of Contractor, if Contractor determines the documents or information are subject to disclosure and the State does not exercise its rights described in Section *CONTRACTOR'S CONFIDENTIAL INFORMATION*(f), or if the State is unsuccessful in defending its rights as described in Section *CONTRACTOR'S CONFIDENTIAL INFORMATION*(f).

Data Security Standards

Data Security: The Contractor at a minimum shall protect and maintain the security of data traveling its network in accordance with generally accepted industry practices.

- Any Personally Identifiable Information must be protected. All data must be classified in accordance with the Statewide Information Security Manual, https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf

- Additionally, data must be disposed of in accordance with the State's Information Disposal and Media Sanitation policy, 09-10-NJOIT.

- Data usage, storage, and protection is subject to all applicable federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for Health Insurance Portability and Accountability Act of 1996

(HIPAA), Personally Identifiable Information (PII), Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, N.J.S.A. 54:50-8, New Jersey Identity Theft Prevention Act, N.J.S.A. 56:11-44 et. seq., the federal Drivers' Privacy Protection Act of 1994, Pub.L.103-322, and the confidentiality requirements of N.J.S.A. 39:2-3.4. Contractor shall also conform to Payment Card Industry (PCI) Data Security Standard.

Data Transmission: The Contractor must only transmit or exchange State of New Jersey data with other parties when expressly requested in writing and permitted by and in accordance with requirements of the State of New Jersey. The Contractor shall only transmit or exchange data with the State of New Jersey or other parties through secure means supported by current technologies. The Contractor must encrypt all data defined as personally identifiable or confidential by the State of New Jersey or applicable law, regulation or standard during any transmission or exchange of that data.

Data Storage: All data provided by the State of New Jersey or State data obtained by the Contractor in the performance of the Contract must be stored, processed, and maintained solely in accordance with a project plan and system topology approved by the State Contract Manager. No State data shall be processed on or transferred to any device or storage medium including portable media, smart devices and/or USB devices, unless that device or storage medium has been approved in advance in writing by the State Project Manager. The Contractor shall encrypt all data at rest defined as personally identifiable information by the State of New Jersey or applicable law, regulation or standard. The Contractor shall not store or transfer State of New Jersey data outside of the United States.

Data Scope: All provisions applicable to State data include data in any form of transmission or storage, including but not limited to: database files, text files, backup files, log files, XML files, and printed copies of the data.

Data Re-Use: All State data shall be used expressly and solely for the purposes enumerated in the Contract. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Contractor. No State data of any kind shall be transmitted, exchanged or otherwise passed to other contractors or interested parties except on a case-by-case basis as specifically agreed to in writing by the State Contract Manager.

Data Breach: Unauthorized Release Notification: The Contractor must comply with all applicable State and Federal laws that require the notification of individuals in the event of unauthorized release of personally identifiable information or other event requiring notification. In the event of a breach of any of the Contractor's security obligations or other event requiring notification under applicable law ("Notification Event"), the Contractor shall assume responsibility for informing the State Contract Manager within 24 hours and all such individuals in accordance with applicable law and to indemnify, hold harmless and defend the State of New Jersey, its officials, and employees from and against any claims, damages, or other harm related to such Notification Event. All communications must be coordinated with the State of New Jersey.