State of New Jersey
Office of Information Technology

File Transfer Guide

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.

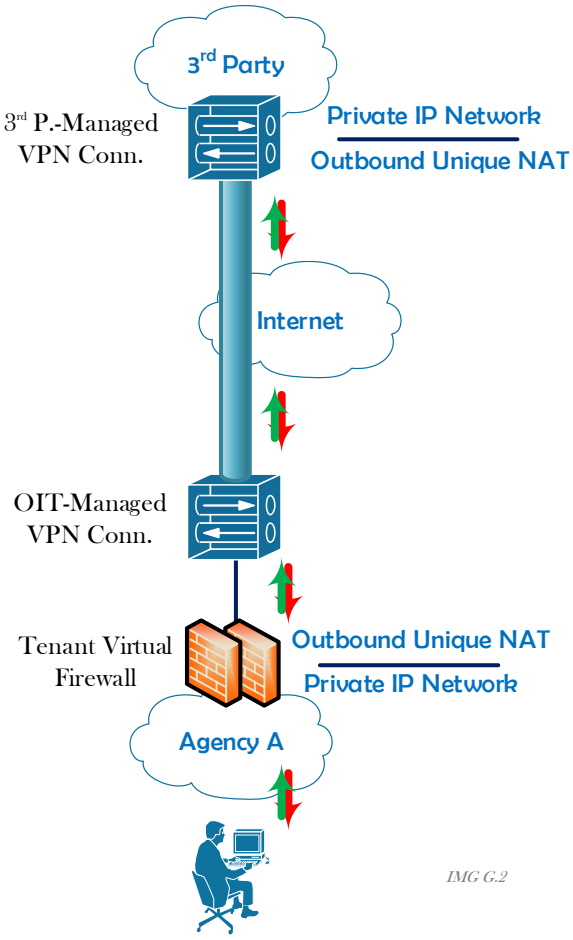
The contractor must work with the sponsoring agency and OIT to establish an Extranet Partner relationship. The State of New Jersey and the Contractor will be required to follow the State's Extranet Policy and Procedure, and complete the application form, MOU, operational form and security controls assessment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

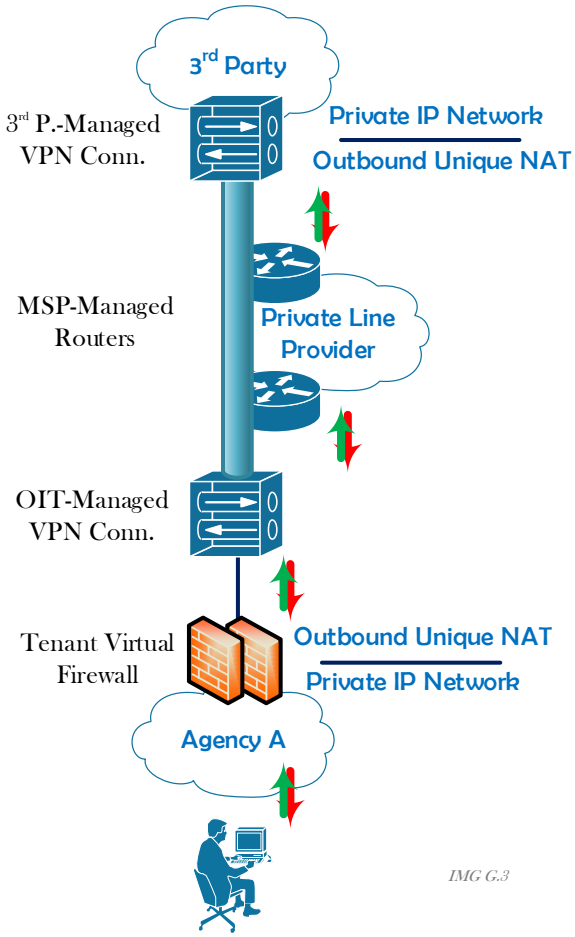


IMG G.2

Extranet Specifics and Topology (Bronze)

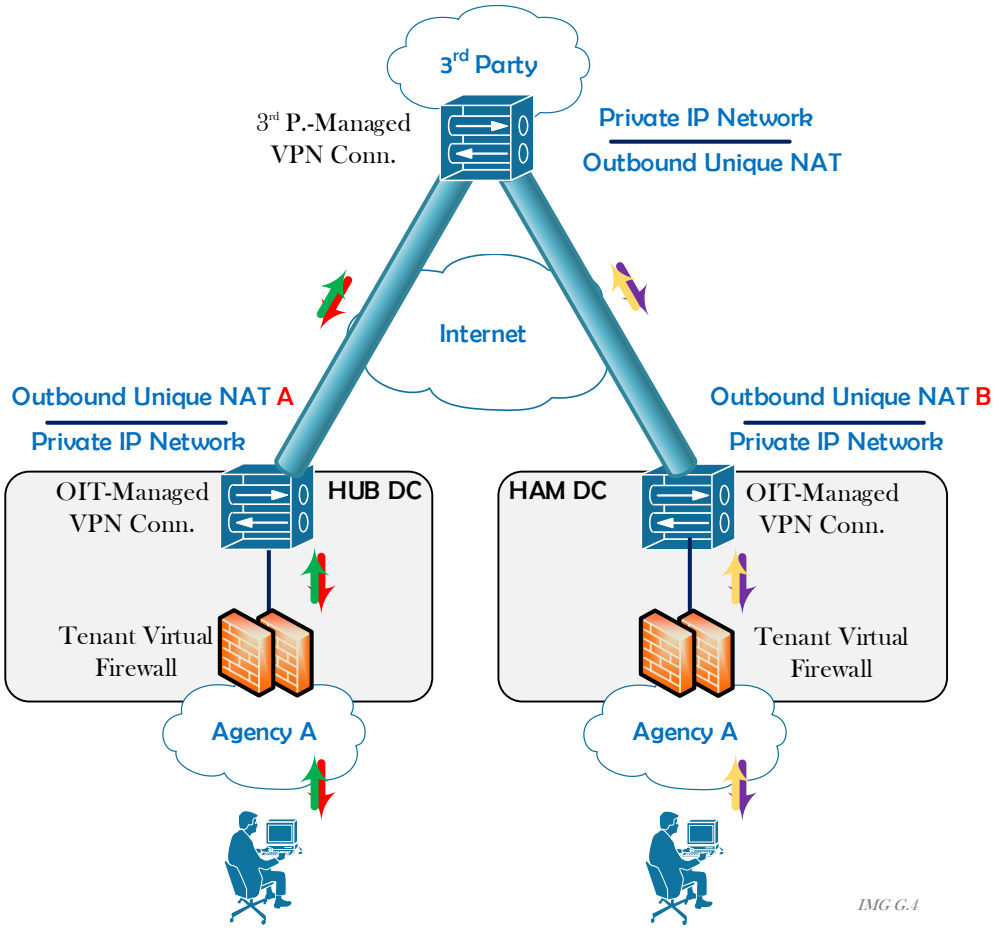
- Various IPSec configuration parameters are supported and should at a minimum meet the recommended values as defined by NJOIT's GSN Technical Architects.
- Bandwidth over the Internet is not guaranteed.
- Internet instability may cause disruption of this tunnel, therefore this Extranet model is considered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

EXHIBIT A



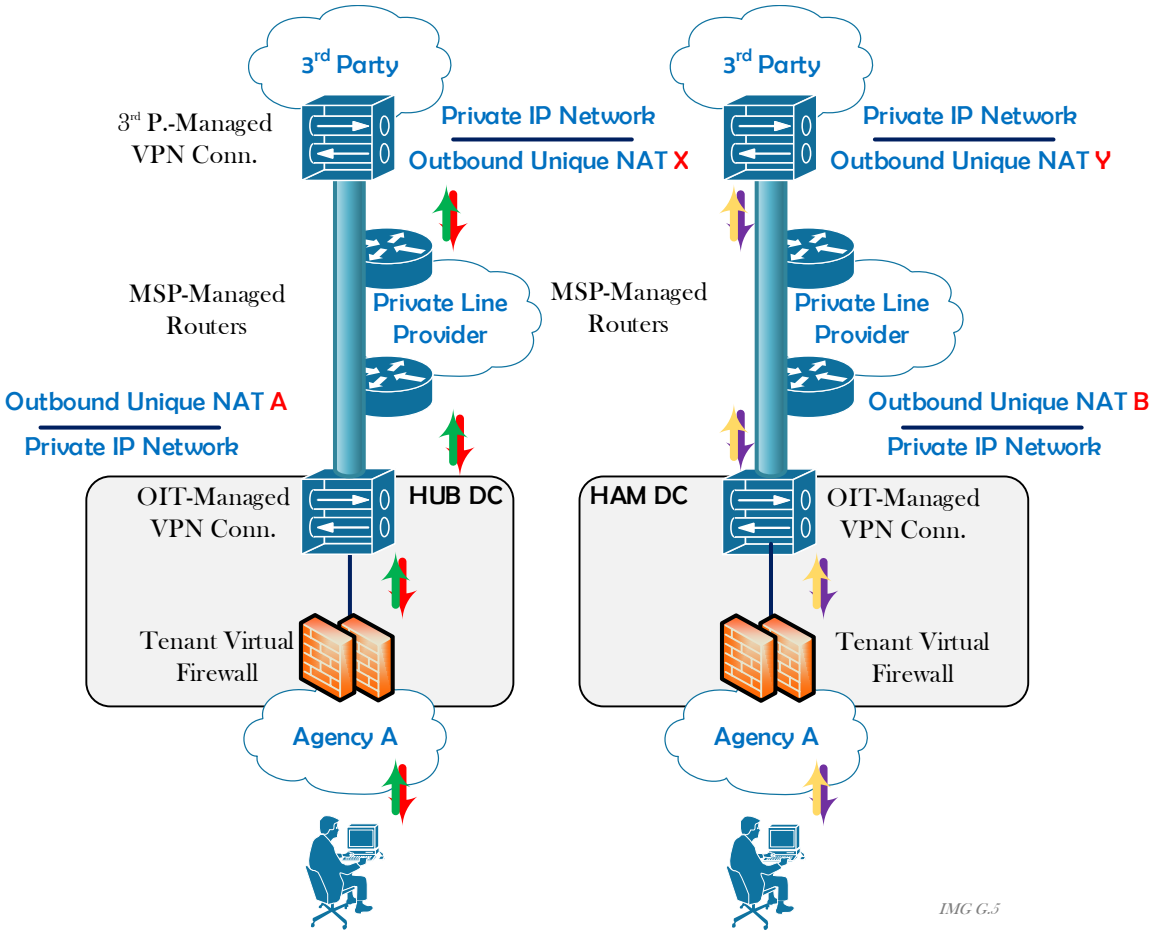
Extranet Specifics and Topology (Silver)

- 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 (non-IBM Mainframe).

Asynchronous:

1) The State of New Jersey's MOVEit Cloud is a supported option for non-automated or "ad-hoc" file exchange with State of New Jersey.

2) The State of New Jersey's MOVEit Cloud Automation 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 (https://csrc.nist.gov/publications/detail/sp/800-47/rev-1/final)

DATA CONFIDENTIALITY AND SECURITY

The Vendor {Contractor} must provide a Security Plan.

The Security Plan shall address administrative, physical, and technical security controls, along with the privacy safeguards that are to be implemented as they relate to the scope of the engagement and the broader Vendor {Contractor's} information security program. The control areas to be addressed include:

SECURITY PLAN

The Vendor {Contractor} shall submit a detailed Security Plan that addresses the Vendor's {Contractor's} approach to meeting each applicable security requirement outlined below, to the State, no later than 30 days after the award of the Blanket P.O. The State approval of the Security Plan shall be set forth in writing. In the event that the State reasonably rejects the Security Plan after providing the Vendor {Contractor} an opportunity to cure, the Director may terminate the Blanket P.O. pursuant to the SSTC.

INFORMATION SECURITY PROGRAM MANAGEMENT

The Vendor {Contractor} shall establish and maintain a framework to provide assurance that information security strategies are aligned with and support the State's business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, in an effort to manage risk. Information security program management shall include, at a minimum, the following:

A. Establishment of a management structure with clear reporting paths and explicit responsibility for information security;
B. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed in sections below;
C. Development and maintenance of relationships with external organizations to stay abreast of current and emerging security issues and for assistance, when applicable; and
D. Independent review of the effectiveness of the Vendor's {Contractor's} information security program.

COMPLIANCE

The Vendor {Contractor} shall develop and implement processes to ensure its compliance with all statutory, regulatory, contractual, and internal policy obligations applicable to this Blanket P.O. Examples include but are not limited to General Data Protection Regulation (GDPR), Payment Card Industry Data Security Standard (PCI DSS), Health Insurance Portability and Accountability Act of 1996 (HIPAA), IRS-1075. Vendor {Contractor} shall timely update its processes as applicable standards evolve.

A. Within ten (10) days after award, the Vendor {Contractor} shall provide the State with contact information for the individual or individuals responsible for maintaining a control framework that captures statutory, regulatory, contractual, and policy requirements relevant to the organization's programs of work and information systems;
B. Throughout the solution development process, Vendor {Contractor} shall implement processes to ensure security assessments of information systems are conducted for all significant development and/or acquisitions, prior to information systems being placed into production; and
C. The Vendor {Contractor} shall also conduct periodic reviews of its information systems on a defined frequency for compliance with statutory, regulatory, and contractual requirements. The Vendor {Contractor} shall document the results of any such reviews.

PERSONNEL SECURITY

The Vendor {Contractor} shall implement processes to ensure all personnel having access to relevant State information have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner. Workforce security controls shall include, at a minimum:

A. Position descriptions that include appropriate language regarding each role's security requirements;
B. To the extent permitted by law, employment screening checks are conducted and successfully passed for all personnel prior to beginning work or being granted access to information assets;
C. Rules of behavior are established and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to information and information systems;
D. Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate;
E. Vendor {Contractor} disables system access for terminated personnel and collects all organization owned assets prior to the individual's departure; and
F. Procedures are implemented that ensure all personnel are aware of their duty to protect information assets and their responsibility to immediately report any suspected information security incidents.

SECURITY AWARENESS AND TRAINING

The Vendor {Contractor} shall provide periodic and on-going information security awareness and training to ensure personnel are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory, regulatory, contractual, and policy requirements that are intended to protect information systems and State Confidential Information from a loss of confidentiality, integrity, availability and privacy. Security awareness and training shall include, at a minimum:

A. Personnel are provided with security awareness training upon hire and at least annually, thereafter;

B. Security awareness training records are maintained as part of the personnel record;
C. Role-based security training is provided to personnel with respect to their duties or responsibilities (e.g. network and systems administrators require specific security training in accordance with their job functions); and
D. Individuals are provided with timely information regarding emerging threats, best practices, and new policies, laws, and regulations related to information security.

RISK MANAGEMENT

The Vendor {Contractor} shall establish requirements for the identification, assessment, and treatment of information security risks to operations, information, and/or information systems. Risk management requirements shall include, at a minimum:

A. An approach that categorizes systems and information based on their criticality and sensitivity;
B. An approach that ensures risks are identified, documented and assigned to appropriate personnel for assessment and treatment;
C. Risk assessments shall be conducted throughout the lifecycles of information systems to identify, quantify, and prioritize risks against operational and control objectives and to design, implement, and exercise controls that provide reasonable assurance that security objectives will be met; and
D. A plan under which risks are mitigated to an acceptable level and remediation actions are prioritized based on risk criteria and timelines for remediation are established. Risk treatment may also include the acceptance or transfer of risk.

PRIVACY

A. Data Ownership. The State is the data owner. Vendor {Contractor} shall not obtain any right, title, or interest in any of the data furnished by the State, or information derived from or based on State data.

B. Data usage, storage, and protection of PII and State Confidential Information, as defined in Section 5.9 are subject to all applicable international, federal and state statutory and regulatory requirements, as amended from time to time, including, without limitation, those for HIPAA, Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075), New Jersey State tax confidentiality statute, the New Jersey Privacy Notice found at NJ.gov, 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. Vendor {Contractor} shall also conform to PCI DSS, where applicable.

C. Security: Vendor {Contractor} agrees to take appropriate administrative, technical and physical safeguards reasonably designed to protect the security, privacy, confidentiality, and integrity of user information. Vendor {Contractor} shall ensure that PII and other State Confidential Information is secured and encrypted during transmission or at rest.

D. Data Transmission: The Vendor {Contractor} shall 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 Blanket P.O. or the State of New Jersey. The Vendor {Contractor} shall only transmit or exchange data with the State of New Jersey or other parties through secure means supported by current technologies. The Vendor {Contractor} shall encrypt all PII and other State Confidential Information as defined by the State of New Jersey or applicable law, regulation or standard during any transmission or exchange of that data.

E. Data Storage: All data provided by the State of New Jersey or State data obtained by the Vendor {Contractor} in the performance of the Blanket P.O. 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 Contract Manager. The Vendor {Contractor} must not store or transfer State of New Jersey data outside of the United States.

F. Data Re-Use: All State data shall be used expressly and solely for the purposes enumerated in the Blanket P.O. Data shall not be distributed, repurposed or shared across other applications, environments, or business units of the Vendor {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.

G. Data Breach: In the event of any actual, probable or reasonably suspected breach of security, or any unauthorized access to or acquisition, use, loss, destruction, compromise, alteration or disclosure of any PII (each, a security breach) that may concern any State Confidential Information or PII, Vendor {Contractor} shall: (a) notify the State immediately of such breach, but in no event later than 24 hours after such security breach; (b) designate a single individual employed by Vendor {Contractor} who shall be available to the State 24 hours per day, seven (7) days per week as a contact regarding Vendor's {Contractor's} obligations under Section X (Incident Response); (c) not provide any other notification or provide any disclosure to the public regarding such security breach without the prior written consent of the State, unless required to provide such notification or to make such disclosure pursuant to any applicable law, regulation, rule, order, court order, judgment, decree, ordinance, mandate or other request or requirement now or hereafter in effect, of any applicable governmental authority or law enforcement agency in any jurisdiction worldwide (in which case Vendor {Contractor} shall consult with the State and reasonably cooperate with the State to prevent any notification or disclosure concerning any PII, security breach, or other State Confidential Information); (d) assist the State in investigating, remedying and taking any other action the State deems necessary regarding any security breach and any dispute, inquiry, or claim that concerns the security breach; (e) follow all instructions provided by the State relating to the State Confidential Information affected or potentially affected by the security breach; (f) take such actions as necessary to prevent future security breaches; and (g) unless prohibited by an applicable statute or court order, notify the State of any third party legal process relating to any security breach including, at a minimum, any legal process initiated by any governmental entity (foreign or domestic).

H. Minimum Necessary. Vendor {Contractor} shall ensure that PII and other State Confidential Information requested represents the minimum necessary information for the services as described in this Bid Solicitation and, unless otherwise agreed to in writing by the State, that only necessary individuals or entities who are familiar with and bound by the Blanket P.O. will have access to the State Confidential Information in order to perform the work.

I. End of Contract Data Handling: Upon termination/expiration of this Blanket P.O. the Vendor {Contractor} shall first return all State data to the State in a usable format as defined in the Blanket P.O., or in an open standards machine-readable format if not. The Vendor {Contractor} shall then erase, destroy, and render unreadable all Vendor {Contractor} back up copies of State data according to the standards enumerated in accordance with the State's most recent Media Protection policy, https://www.nj.gov/it/docs/ps/NJ_Statewide_Information_Security_Manual.pdf, and certify in writing that these actions have been completed within 30 days after the termination/expiration of the Blanket P.O. or within seven (7) days of the request of an agent of the State whichever should come first.

J. In the event of loss of any State data or records where such loss is due to the intentional act, omission, or negligence of the Vendor {Contractor} or any of its subcontractors or agents, the Vendor {Contractor} shall be responsible for recreating such lost data in the manner and on the schedule set by the State Contract Manager. The Vendor {Contractor} shall ensure that all data is backed up and is recoverable by the Vendor {Contractor}. In accordance with prevailing federal or state law or regulations, the Vendor {Contractor} shall report the loss of non-public data.

ASSET MANAGEMENT

The Vendor {Contractor} shall implement administrative, technical, and physical controls necessary to safeguard information technology assets from threats to their confidentiality, integrity, or availability, whether internal or external, deliberate or accidental. Asset management controls shall include at a minimum:

A. Information technology asset identification and inventory;
B. Assigning custodianship of assets; and
C. Restricting the use of non-authorized devices.

SECURITY CATEGORIZATION

The Vendor {Contractor} shall implement processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact in the event that there is a loss of confidentiality, integrity, availability, or breach of privacy. Information classification and system categorization includes labeling and handling requirements. Security categorization controls shall include the following, at a minimum:

A. Implementing a data protection policy;

B. Classifying data and information systems in accordance with their sensitivity and criticality;
C. Masking sensitive data that is displayed or printed; and
D. Implementing handling and labeling procedures.

MEDIA PROTECTION

The Vendor {Contractor} shall establish controls to ensure data and information, in all forms and mediums, are protected throughout their lifecycles based on their sensitivity, value, and criticality, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on the Vendor {Contractor}, business partners, or individuals. Media protections shall include, at a minimum:

A. Media storage/access/transportation;
B. Maintenance of sensitive data inventories;
C. Application of cryptographic protections;
D. Restricting the use of portable storage devices;
E. Establishing records retention requirements in accordance with business objectives and statutory and regulatory obligations; and
F. Media disposal/sanitization.

CRYPTOGRAPHIC PROTECTIONS

The Vendor {Contractor} shall employ cryptographic safeguards to protect sensitive information in transmission, in use, and at rest, from a loss of confidentiality, unauthorized access, or disclosure. Cryptographic protections shall include at a minimum:

A. Using industry standard encryption algorithms;
B. Establishing requirements for encryption of data in transit;
C. Establishing requirements for encryption of data at rest; and
D. Implementing cryptographic key management processes and controls.

ACCESS MANAGEMENT

The Vendor {Contractor} shall establish security requirements and ensure appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the Vendor's {Contractor's} information systems that contain or could be used to access State data. Access management plan shall include the following features:

A. Ensure the principle of least privilege is applied for specific duties and information systems (including specific functions, ports, protocols, and services), so processes operate at privilege levels no higher than necessary to accomplish required organizational missions and/or functions;
B. Implement account management processes for registration, updates, changes and de-provisioning of system access;
C. Apply the principles of least privilege when provisioning access to organizational assets;
D. Provision access according to an individual's role and business requirements for such access;

E. Implement the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;
F. Conduct periodic reviews of access authorizations and controls.

IDENTITY AND AUTHENTICATION

The Vendor {Contractor} shall establish procedures and implement identification, authorization, and authentication controls to ensure only authorized individuals, systems, and processes can access the State's information and Vendor's {Contractor's} information and information systems. Identity and authentication provides a level of assurance that individuals who log into a system are who they say they are. Identity and authentication controls shall include, at a minimum:

A. Establishing and managing unique identifiers (e.g. User-IDs) and secure authenticators (e.g. passwords, biometrics, personal identification numbers, etc.) to support nonrepudiation of activities by users or processes; and
B. Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the Vendor's {Contractor's} systems.

REMOTE ACCESS

The Vendor {Contractor} shall strictly control remote access to the Vendor's {Contractor's} internal networks, systems, applications, and services. Appropriate authorizations and technical security controls shall be implemented prior to remote access being established. Remote access controls shall include at a minimum:

A. Establishing centralized management of the Vendor's {Contractor's} remote access infrastructure;
B. Implementing technical security controls (e.g. encryption, multi-factor authentication, IP whitelisting, geo-fencing); and
C. Training users in regard to information security risks and best practices related remote access use.

SECURITY ENGINEERING AND ARCHITECTURE

The Vendor {Contractor} shall employ security engineering and architecture principles for all information technology assets, and such principles shall incorporate industry recognized leading security practices and sufficiently address applicable statutory and regulatory obligations. Applying security engineering and architecture principles shall include:

A. Implementing configuration standards that are consistent with industry-accepted system hardening standards and address known security vulnerabilities for all system components;
B. Establishing a defense in-depth security posture that includes layered technical, administrative, and physical controls;
C. Incorporating security requirements into the systems throughout their life cycles;
D. Delineating physical and logical security boundaries;

E. Tailoring security controls to meet organizational and operational needs;
F. Performing threat modeling to identify use cases, threat agents, attack vectors, and attack patterns as well as compensating controls and design patterns needed to mitigate risk;
G. Implementing controls and procedures to ensure critical systems fail-secure and fail-safe in known states; and
H. Ensuring information system clock synchronization.

CONFIGURATION MANAGEMENT

The Vendor {Contractor} shall ensure that baseline configuration settings are established and maintained in order to protect the confidentiality, integrity, and availability of all information technology assets. Secure configuration management shall include, at a minimum:

A. Hardening systems through baseline configurations; and
B. Configuring systems in accordance with the principle of least privilege to ensure processes operate at privilege levels no higher than necessary to accomplish required functions.

ENDPOINT SECURITY

The Vendor {Contractor} shall ensure that endpoint devices are properly configured, and measures are implemented to protect information and information systems from a loss of confidentiality, integrity, and availability. Endpoint security shall include, at a minimum:

A. Maintaining an accurate and updated inventory of endpoint devices;
B. Applying security categorizations and implementing appropriate and effective safeguards on endpoints;
C. Maintaining currency with operating system and software updates and patches;
D. Establishing physical and logical access controls;
E. Applying data protection measures (e.g. cryptographic protections);
F. Implementing anti-malware software, host-based firewalls, and port and device controls;
G. Implementing host intrusion detection and prevention systems (HIDS/HIPS) where applicable;
H. Restricting access and/or use of ports and I/O devices; and
I. Ensuring audit logging is implemented and logs are reviewed on a continuous basis.

ICS/SCADA/OT SECURITY

The Vendor {Contractor} shall implement controls and processes to ensure risks, including risks to human safety, are accounted for and managed in the use of Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA) systems and Operational Technologies (OT). ICS/SCADA/OT Security requires the application of all of the enumerated control areas in this Bid Solicitation, including, at a minimum:

A. Conducting risk assessments prior to implementation and throughout the lifecycles of ICS/SCADA/OT assets;
B. Developing policies and standards specific to ICS/SCADA/OT assets;
C. Ensuring the secure configuration of ICS/SCADA/OT assets;
D. Segmenting ICS/SCADA/OT networks from the rest of the Vendor's {Contractor's} networks;
E. Ensuring least privilege and strong authentication controls are implemented
F. Implementing redundant designs or failover capabilities to prevent business disruption or physical damage; and
G. Conducting regular maintenance on ICS/SCADA/OT systems.

INTERNET OF THINGS SECURITY

The Vendor {Contractor} shall implement controls and processes to ensure risks are accounted for and managed in the use of Internet of Things (IoT) devices including, but not limited to, physical devices, vehicles, appliances and other items embedded with electronics, software, sensors, actuators, and network connectivity which enables these devices to connect and exchange data. IoT. IoT security shall include, at a minimum, the following:

A. Developing policies and standards specific to IoT assets;
B. Ensuring the secure configuration of IoT assets;
C. Conducting risk assessments prior to implementation and throughout the lifecycles of IoT assets;
D. Segmenting IoT networks from the rest of the Vendor's {Contractor's} networks; and
E. Ensuring least privilege and strong authentication controls are implemented.

MOBILE DEVICE SECURITY

The Vendor {Contractor} shall establish administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes. Mobile device security shall include, at a minimum, the following:

A. Establishing requirements for authorization to use mobile devices for organizational business purposes;
B. Establishing Bring Your Own Device (BYOD) processes and restrictions;
C. Establishing physical and logical access controls;
D. Implementing network access restrictions for mobile devices;
E. Implementing mobile device management solutions to provide centralized management of mobile devices and to ensure technical security controls (e.g. encryption, authentication, remote-wipe, etc.) are implemented and updated as necessary;
F. Establishing approved application stores from which applications can be acquired;
G. Establishing lists approved applications that can be used; and
H. Training of mobile device users regarding security and safety.

NETWORK SECURITY

The Vendor {Contractor} shall implement defense-in-depth and least privilege strategies for securing the information technology networks that it operates. To ensure information technology resources are available to authorized network clients and protected from unauthorized access, the Vendor {Contractor} shall:

A. Include protection mechanisms for network communications and infrastructure (e.g. layered defenses, denial of service protection, encryption for data in transit, etc.);
B. Include protection mechanisms for network boundaries (e.g. limit network access points, implement firewalls, use Internet proxies, restrict split tunneling, etc.);
C. Control the flow of information (e.g. deny traffic by default/allow by exception, implement Access Control Lists, etc.); and
D. Control access to the Vendor's {Contractor's} information systems (e.g. network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

CLOUD SECURITY

The Vendor {Contractor} shall establish security requirements that govern the use of private, public, and hybrid cloud environments to ensure risks associated with a potential loss of confidentiality, integrity, availability, and privacy are managed. This shall ensure, at a minimum, the following:

A. Security is accounted for in the acquisition and development of cloud services;
B. The design, configuration, and implementation of cloud-based applications, infrastructure and system-system interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;
C. Security roles and responsibilities for the Vendor {Contractor} and the cloud provider are delineated and documented; and
D. Controls necessary to protect sensitive data in public cloud environments are implemented.

CHANGE MANAGEMENT

The Vendor {Contractor} shall establish controls required to ensure change is managed effectively. Changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the Vendor {Contractor} with the ability to handle changes in a controlled, predictable, and repeatable manner, and to identify, assess, and minimize the risks to operations and security. Change management controls shall include, at a minimum, the following:

A. Notifying all stakeholder of changes;
B. Conducting a security impact analysis and testing for changes prior to rollout; and
C. Verifying security functionality after the changes have been made.

MAINTENANCE

The Vendor {Contractor} shall implement processes and controls to ensure that information assets are properly maintained, thereby minimizing the risks from emerging information security threats and/or the potential loss of confidentiality, integrity, or availability due to system failures. Maintenance security shall include, at a minimum, the following:

A. Conducting scheduled and timely maintenance;
B. Ensuring individuals conducting maintenance operations are qualified and trustworthy; and
C. Vetting, escorting and monitoring third-parties conducting maintenance operations on information technology assets.

THREAT MANAGEMENT

The Vendor {Contractor} shall establish effective communication protocols and processes to collect and disseminate actionable threat intelligence, thereby providing component units and individuals with the information necessary to effectively manage risk associated with new and emerging threats to the organization's information technology assets and operations. Threat management includes, at a minimum:

A. Developing, implementing, and governing processes and documentation to facilitate the implementation of a threat awareness policy, as well as associated standards, controls and procedures.
B. Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.

VULNERABILITY AND PATCH MANAGEMENT (VU)

The Vendor {Contractor} shall implement proactive vulnerability identification, remediation, and patch management practices to minimize the risk of a loss of confidentiality, integrity, and availability of information system, networks, components, and applications. Vulnerability and patch management practices shall include, at a minimum, the following:

A. Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of systems and information, and the risks associated with a loss of confidentiality, integrity, availability, and/or privacy;
B. Maintaining software and operating systems at the latest vendor-supported patch levels;
C. Conducting penetration testing and red team exercises; and
D. Employing qualified third-parties to periodically conduct Independent vulnerability scanning, penetration testing, and red-team exercises.

CONTINUOUS MONITORING

The Vendor {Contractor} shall implement continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability, privacy and safety of information and information systems through timely collection and review of security-related event logs. Continuous monitoring practices shall include, at a minimum, the following:

A. Centralizing the collection and monitoring of event logs;
B. Ensuring the content of audit records includes all relevant security event information;
C. Protecting of audit records from tampering; and
D. Detecting, investigating, and responding to incidents discovered through monitoring.

SYSTEM DEVELOPMENT AND ACQUISITION

The Vendor {Contractor} shall establish security requirements necessary to ensure that systems and application software programs developed by the Vendor {Contractor} or third-parties (e.g. vendors, contractors, etc.) perform as intended to maintain information confidentiality, integrity, and availability, and the privacy and safety of individuals. System development and acquisition security practices shall include, at a minimum, the following:

A. Secure coding;
B. Separation of development, testing, and operational environments;
C. Information input restrictions;
D. Input data validation;
E. Error handling;
F. Security testing throughout development;
G. Restrictions for access to program source code; and
H. Security training of software developers and system implementers.

PROJECT AND RESOURCE MANAGEMENT

The Vendor {Contractor} shall ensure that controls necessary to appropriately manage risks are accounted for and implemented throughout the System Development Life Cycle (SDLC). Project and resource management security practices shall include, at a minimum:

A. Defining and implementing security requirements;
B. Allocating resources required to protect systems and information; and
C. Ensuring security requirements are accounted for throughout the SDLC.

CAPACITY AND PERFORMANCE MANAGEMENT

The Vendor {Contractor} shall implement processes and controls necessary to protect against avoidable impacts to operations by proactively managing the capacity and performance of its critical technologies and supporting infrastructure. Capacity and performance management practices shall include, at a minimum, the following:

A. Ensuring the availability, quality, and adequate capacity of compute, storage, memory and network resources are planned, prepared, and measured to deliver the required system performance and future capacity requirements; and
B. Implementing resource priority controls to prevent or limit Denial of Service (DoS) effectiveness.

THIRD PARTY MANAGEMENT

The Vendor {Contractor} shall implement processes and controls to ensure that risks associated with third-parties (e.g. vendors, contractors, business partners, etc.) providing information technology equipment, software, and/or services are minimized or avoided. Third party management processes and controls shall include, at a minimum:

A. Tailored acquisition strategies, contracting tools, and procurement methods for the purchase of systems, system components, or system service from suppliers;
B. Due diligence security reviews of suppliers and third parties with access to the Vendor's {Contractor's} systems and sensitive information;
C. Third party interconnection security; and
D. Independent testing and security assessments of supplier technologies and supplier organizations.

PHYSICAL AND ENVIRONMENTAL SECURITY

The Vendor {Contractor} shall establish physical and environmental protection procedures that limit access to systems, equipment, and the respective operating environments, to only authorized individuals. The Vendor {Contractor} ensures appropriate environmental controls in facilities containing information systems and assets, to ensure sufficient environmental conditions exist to avoid preventable hardware failures and service interruptions. Physical and environmental controls shall include, at a minimum, the following:

A. Physical access controls (e.g. locks, security gates and guards, etc.);
B. Visitor controls;
C. Security monitoring and auditing of physical access;
D. Emergency shutoff;
E. Emergency power;
F. Emergency lighting;
G. Fire protection;
H. Temperature and humidity controls;
I. Water damage protection; and
J. Delivery and removal of information assets controls.

CONTINGENCY PLANNING

The Vendor {Contractor} shall develop, implement, test, and maintain a contingency plan to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the Vendor {Contractor}. The plan shall address the following:

A. Backup and recovery strategies;
B. Continuity of operations;
C. Disaster recovery; and
D. Crisis management.

INCIDENT RESPONSE

The Vendor {Contractor} shall maintain an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities shall include, at a minimum, the following:

A. Information security incident reporting awareness;
B. Incident response planning and handling;
C. Establishment of an incident response team;
D. Cybersecurity insurance;
E. Contracts with external incident response services specialists; and
F. Contacts with law enforcement cybersecurity units.