Appendix D to
09-11-P1-NJOIT

P.O. Box 212 www.nj.gov/it/ps/
300 Riverview Plaza
Trenton, NJ 08625-0212

STATE OF NEW JERSEY
Security Controls Assessment Checklist

Agency/Business (Extranet) Entity ____________________

Response ____________________

Agency

Agency Name: ____________________

Application Name: ____________________

Point of Contact: ____________________

Telephone Number: ____________________

Date: ____________________

Business (Extranet) Entity

Name: ____________________

Point of Contact: ____________________

Telephone Number: ____________________

Email Address: ____________________

Security Point of Contact: ____________________

Telephone Number: ____________________

Email Address: ____________________

No.	Doc.	Security Control Item	Security Description/Requirements	Response/Acknowledgement
1	T&C	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 & 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.	
2	T&C		Regulations and security requirements – How the Contractor will address security requirements such as PCI, HIPAA, FISMA and etc.	
3	T&C		System, Administrative and Personnel Security – The security responsibilities 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.	
4	T&C		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.	
5	T&C		Role-based security access – The products and methods provide role-based security, access enforcement and least privilege.	

6	T&C		Account Management – The products and methods identify and control the account types to meet defined regulation and security requirements.	
7	T&C		Password Management – The appropriate password management controls to meet defined regulation or security requirements.	
8	T&C		Logging/Auditing controls – The Contractor's audit control methods and requirements. The controls must address 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 90 days and further preserved offline for the period required by the contract or State and Federal laws and regulations.	
9	T&C		Incident Management – The methods for detecting, reporting and responding to an incident, vulnerabilities and threats. The methods are tested and exercised.	
10	T&C		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.	
11	T&C		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.	
12	T&C		Application Partitioning – Where the Contractor is providing application hosting or development services, the Contractor will have a separate and unique (single tenant) partition.	

13	T&C		Anti-virus/malware controls – The products and methods for anti-virus and malware controls 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.	
14	T&C		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. The Contractor shall 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	
15	T&C		Database – The products and methods for safeguarding the database(s).	
16	T&C		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.	
17	T&C		Server and infrastructure – The products and methods for "hardening" of the hardware's operating systems and software.	
18	T&C		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.	
19	T&C		Transmission – The products and methods on how its system addresses security measures regarding communication transmission, access and message validation.	
20	T&C		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 and intrusions, and for creating audit records within the Contractor’s network.	
21	T&C		Security Audit – The Contractor must allow State-assigned staff full access to all 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.	
22	T&C SOW		Change/Configuration Management and Security Authorization – The Contractor has established a change/configuration methodology, has a baseline configuration and tracks changes to the configuration. The contractor must 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.	
23	T&C SOW		Risk Management – The Contractor has established a risk management plan, technical and security risks are identified, reported and mitigated.	
24	T&C SOW		Confidentiality and Non-Disclosure Agreements – When requested, the Contractor and all project staff including subcontractors must complete and sign confidentiality and non-disclosure agreements provided by the State. The Contractor may be required to view yearly security awareness materials and confidentiality training modules provided by the State. Where required, it shall be the Contractor’s responsibility to ensure that any new staff sign the confidentiality agreement(s) and complete the security awareness and confidentiality training modules within one month of the employees’ start date.	
25	T&C SOW		The State reserves the right to obtain, or require the Contractor to obtain, criminal history background checks from the New Jersey State Police for all Contractor and project staff (to protect the State of New Jersey from losses resulting from contractor employee theft, fraud or dishonesty) when requested. If the State exercises this right, the results of the background check(s) must be made available to the State for consideration before the employee is assigned to work on the State’s project. Prospective employees with criminal backgrounds that include cyber-crimes will not	

			be approved to work on State Projects. Refer to the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-12, An Introduction to Computer Security: The NIST Handbook, Section 10.1.3, Filling the Position – Screening and Selecting.	
26	T&C		The Contractor shall disclose to the State of New Jersey a description of its roles and responsibilities related to electronic discovery, litigation holds, discovery searches, and expert testimonies. The Contractor shall disclose its process for responding to subpoenas, service of process, and other legal requests.	
27	T&C	Disaster Recovery Plan	The Contractor is required to submit its Disaster Recovery plan, identifying locations and systems – to ensure that it can continue to satisfy the terms and conditions requirements within 24 hours, in the event its primary location is rendered unusable. The plan must detail how the Contractor will ensure that the primary location and/or systems destroyed in such a disaster would be made available to meet the 24-hour time frame. The Contractor must submit that the plan is tested, and that the plan is reviewed and updated annually.	
28	T&C	Contingency Plan	The Contractor is required to have a contingency plan identifying key personnel, organization units and alternate sites with telecommunications and computers. The plan must be tested. The plan must be reviewed and updated annually.	
29	T&C SOW	System Design	The Contractor shall develop a system that uses a standards-based design that follows the *State of New Jersey Shared IT Architecture*.	
30	T&C		The Contractor shall replicate all State data on its system(s) to a designated State system in a format and frequency as defined in the Contract, or if not defined, in an open standards machine-readable format designated by the NJ Office of Information Technology no less frequently than once a month.	
31	T&C SOW		The State of New Jersey and the Contractor shall identify a collaborative governance structure as part of the design and development of service delivery and service agreements.	
32	T&C SOW		The Contractor shall identify all of its strategic business partners who will be involved in any application development and/or operations.	

33	T&C	Hosting and Backup Services	For “outsourced hosting services,” the Contractor must demonstrate the ability to not only secure the physical application infrastructure utilizing the above mentioned security requirements, but also control and secure physical access to the application hosting facilities and the racks supporting network infrastructure and processing server equipment, web, application and database servers. The backed-up data cannot be commingled with other customer data. If the Contractor is not supplying dedicated hardware resources to host State of New Jersey applications and data, the Contractor must demonstrate its strategy to maintain application and/or stack isolation using commercially available security devices to maintain security zones, routing isolation and access control to infrastructure devices, and access/security logging (AAA) within its infrastructure.	
34	T&C	Extranet Plan	The communication links between the State of New Jersey and the contractor can be through a MPLS cloud (preferred) or IPSEC tunnel over the Internet based upon the connectivity requirements and cost constraints.	
35	T&C		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.	
36	T&C	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 state and federal security guidelines and standards.	
37	T&C SOW	Data Confidentiality	All 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.	
38	T&C SOW		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 the State of New Jersey's written request.	
39	T&C	Data Security Standards	The Contractor at a minimum shall protect and maintain the security of data traveling its network in accordance with generally accepted industry practices.	
40	T&C	Data Security	Any Personally Identifiable Information must be protected. All data must be classified in accordance with the State's Asset Classification and Control policy, 08-04-NJOIT (www.nj.gov/it/ps). Additionally, data must be disposed of in accordance with the State's Information Disposal and Media Sanitation policy, 09-10-NJOIT (www.nj.gov/it/ps).	
41	T&C SOW		Data usage, storage, and protection are 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.	

42	T&C	Data Transmission	The 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 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 shall 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.	
43	T&C	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.	
44	T&C	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.	
45	T&C SOW	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.	

46	T&C SOW	Data Breach	Unauthorized Release Notification: The Contractor shall 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.	
47	T&C	End of Contract Data Handling	Upon termination/expiration of this Contract the Contractor shall first return all State data to the State in a usable format as defined in the Contract, or in an open standards machine-readable format if not. The contractor shall then erase, destroy, and render unreadable all Contractor copies of State data according to the standards enumerated in accordance with the State's most recent Information Disposal and Media Sanitation policy, currently 09-10-NJOIT (www.nj.gov/it/ps) and certify in writing that these actions have been completed within thirty (30) days after the termination/expiration of the Contract or within seven (7) days of the request of an agent of the State whichever shall come first.	
48	T&C	Federal Tax Information	Involving Federal Tax Information (FTI) or Personal Identifiable Information (PII) received from the IRS or validated against IRS FTI/PII the Contractor must adhere to Federal Tax Information Security (Tax Information Security Guidelines for Federal, State, and Local Agencies (IRS Publication 1075 Exhibit 7))	

References

State of New Jersey's RFP Security Control language

Information Security Management ISO 27002:2005 (http://www.iso.org/iso/catalogue_detail?csnumber=50297)

NIST Special Publication 800-53A – Guide for Assessing the Security Controls in Federal Information Systems and Organizations (http://csrc.nist.gov/publications/nistpubs/800-53-Rev3/sp800-53-rev3-final_updated-errata_05-01-2010.pdf.

Glossary

T&C – Terms and conditions for Request for Proposal (RFP), Waivers and GSA Contract covering on-premise, hosting or cloud service

SOW – Statement of Work