NJ TRANSIT

Cyber Security
Contract
Terms and Conditions

Rafi Khan, Chief Information Security Officer
Effective: 10/26/2021

Table of Contents

General Cyber Security Requirements

1. Contractor shall comply with all New Jersey Transit ("NJ TRANSIT") Information Security Policies and Technology Standards as published by NJ TRANSIT at the time of this agreement. New policies and/or changes to existing policies shall be provided to the vendor, at which time all parties shall mutually agree upon adoption schedule and implementation plan and if any change orders are required to address material change to this agreement.

2. Contractor shall provide written acknowledgement of receipt of all policies and appropriate NJ TRANSIT non-disclosure agreements. Contractor shall confirm the distribution of these documents to its employees, consultants, and sub-contractors, as applicable.

Security Standards, Certification, and Accreditation

3. Contractor shall ensure that any products, services and other work products provided are compliant with all NJ TRANSIT Information Security Polices and NIST 800-53 standards and applicable controls referenced herein.

4. ALL NJ Transit systems and applications that support NJ TRANSIT operations must be built in a secure fashion. Systems and applications may be reviewed and approved by NJ TRANSIT's Chief Information Security Officer or designee through the Security Certification and Accreditation ("**SCA**") Process prior to migrating to the production environment.

   4.1 Contractor shall cooperate with and facilitate the successful completion of any Security Accreditation tasks and processes relevant to the services and/or work products provided. A copy of NJ TRANSIT's SCA will be provided.

5. The Contractor and all applicable subcontractors shall use and maintain a structured information security program in conjunction with all goods, services, and work products provided to NJ TRANSIT under this Agreement.

   5.1 The Contractor must supply a Cyber Security Plan **("CSP"),** in conjunction with their corporate information security management system ("**ISMS**") program to fulfill this requirement.

   5.2 The CSP shall be made available to NJ TRANSIT electronically upon its completion as part of the System Development Life Cycle ("**SDLC**").

   5.3 The CSP shall be considered "Confidential" and shall be handled according to NJ TRANSIT's data classification policy.

   5.4 The Contractor shall notify NJT of any changes to its CSP in writing. Changes may not degrade the security posture of the CSP or the products or services included in this agreement.

6. During the SDLC, the Contractor shall provide a responsibility matrix that defines which security controls within the framework are the responsibility of the Contractor and which security controls are the responsibilities of NJ TRANSIT. This requirement may be met as part of the requirements definition and system design phases of the project.

   The Contractor and NJ TRANSIT shall not share responsibilities. The Contractor shall provide the necessary detail, in writing, to make clear the delineation of responsibility. In the case that modifications to technology environments, services, agreements, or other conditions result in changes, or presumed changes, to these responsibilities, the Contractor is required to update this responsibility matrix accordingly and provide to NJ TRANSIT for approval. The Contractor shall review and validate this matrix on an annual basis and provide a validated copy to NJ TRANSIT.

7. Security controls associated with the goods and services provided to NJ TRANSIT under this Agreement, shall be designed, implemented, and maintained in a manner that meets or exceeds the standards and intent established by the NIST Security and Privacy Controls for Federal Information Systems and Organizations SP 800-53 **("NIST SP 800-53")** and/or the NIST Guide to Industrial Control Systems ("ICS") Security SP 800-82 **("NIST SP 800-82")**.

   The Contractor shall comply with all current and future revisions, updates, and approved modifications to NIST 800-53 and NIST 800-82 for the duration of this Agreement to include during the provision of warranty, support, and maintenance periods.

   7.1 Following ISO/IEC 27001 and ISO/IEC 27002 Standards may be accepted in lieu of adherence to NIST SP 800-53 and NIST SP 800-82 controls with approval from NJ TRANSIT's Chief Information Security Officer.

8. Contractor shall follow standards and guidelines referenced within the NIST Cyber Security Framework, SP 800-53, and SP 800-82 where applicable. Where no standard applies, Contractor shall follow industry standards and best practices to ensure that it does not introduce any malware, malicious code, or other cyber security threat to NJ TRANSIT systems and network.

9. Based on emerging threats, new vulnerabilities, and/or a change in cyber security risk threshold, NJ TRANSIT may, at its sole discretion, state additional specific information security-related requirements to reduce specific risks based on the design, specifications, goods, services, and work products provided under this agreement.

   NJ TRANSIT shall collaborate with the Contractor to determine a mutually acceptable time to respond to these requirements and to implement any new compensating controls. Where applicable, Contractor shall also provide a reasonable cost proposal for the development and implementation of new controls.

10. The Contractor is required to provide reasonably sufficient evidence of compliance with the information security framework(s) and security control standards for goods, services, and work products provided to NJ TRANSIT under this Agreement.

    10.1 Relevant policies and procedural documentation shall be readily available and furnished upon request, subject to contractor's standard document review process (i.e. on site, closed-door, mutual non-disclosure agreement ("NDA"), etc.).

    10.2 A representative sampling of security operations procedure records shall be readily available and furnished upon request, subject to contractor's standard document review process (i.e. on site, closed-door, mutual NDA, etc.).

    10.3 Technical standards for implementation, maintenance, and monitoring of any systems delivered as work product, or used to provide, services to NJ TRANSIT shall be furnished upon request, subject to contractor’s standard document review process (i.e. on site, closed-door, mutual NDA, etc.).

10.4 Contractor shall provide a response to risk assessment questionnaire(s) as reasonably required assessing the security posture of the Contractor goods, services, and work products provided to NJ TRANSIT, no later than forty-five (45) days from receipt, and at no cost to NJ TRANSIT.

11. The Contractor shall, at its own expense, have a comprehensive information security assessment conducted of all infrastructure, systems, applications, resources, processes, and physical premises used to provide goods, services, and work products to NJ TRANSIT by a qualified 3rd party information security firm. This assessment is to be conducted minimally on an annual basis and upon significant change(s) to elements of the goods, services, and work products relevant to NJ TRANSIT. The contract shall base the assessment on current versions of the following items, as applicable:

11.1 Contractor’s CSP
11.2 NIST Cybersecurity Framework
11.3 NIST Risk Management Framework
11.4 NIST Privacy Framework
11.5 NIST Security and Privacy Controls for Information Systems and Organizations - SP 800-53
11.6 NIST Guide to Industrial Control System (ICS) Security - SP 800-82
11.7 Future revisions of the frameworks and controls listed in items 10.1 thru 10.6 shall apply.

12. When requested, Contractor agrees to provide evidence of an independent IT security review or audit commensurate with the security requirements of the project. This audit must be completed within a reasonable amount of time, as mutually agreed upon by the Contractor and NJ TRANSIT. Cost for such activities shall be mutually agreed upon.

12.1 NJ TRANSIT reserves the right to audit the IT infrastructure and information security controls and processes of the Contractor and to perform relevant tests to ensure that it is compliant with NJ TRANSIT Policies and Standards. Contractor shall permit NJ TRANSIT or its designee to perform an IT audit, including an audit of physical security of any Contractor premises applicable to the engagement, and will cooperate and furnish all requested materials in a timely manner.

12.2 NJ TRANSIT reserves the right to conduct a reasonable review of the qualifications and independence of third-party information security firms selected by the Contractor for information security assessments. Assessment services conducted by firms found unacceptable by NJ TRANSIT in regard to qualifications and/or independence shall not be interpreted as satisfying this requirement.

13. The Contractor shall permit NJ TRANSIT, or its designee, to conduct a risk assessment of planned and/or delivered goods, services, and work products prior to contract execution, annually thereafter or upon a relevant/significant change to the service. The risk assessment process may include, at the discretion of the NJ TRANSIT Chief Information Security Officer or his/her delegate, some or all of the following:

13.1 Review of policy, process, and technical documentation.
13.2 Distribution of one or more information security questionnaires the Contractor is required to complete.
13.3 Interview(s) with relevant Contractor personnel
13.4 Technical testing, such as vulnerability scanning
13.5 Inspection of systems, technology components, and/or configurations
13.6 Physical inspection of facilities

14. NJ TRANSIT may accept a risk assessment conducted by a qualified third-party information security firm as satisfactory fulfillment of requirement 12. Such acceptance shall not to be interpreted as an established precedent for future information requests or for risk assessment processes.

15. The Contractor shall permit reasonable observation of services conducted, and inspection of goods, services, and work products provided, for NJ TRANSIT. Access to facilities, infrastructure, systems, personnel, application code, etc. will not be restricted in a manner to impede the purpose and scope of this observation/inspection. The scope of this observation/inspection is limited to the satisfaction of the requirements/conditions contained herein; issues identified in this regard will require reasonable remedy by the Contractor as a condition of the Agreement.

16. It is the responsibility of the Contractor to notify NJ TRANSIT of any additional party subcontracted by the Contractor to provide goods, services, or work products under this agreement. This notification shall take place prior to initial contract/agreement execution and prior to any party being subcontracted by the Contractor for providing services to NJ TRANSIT after the contract/agreement is in place.

17. It is the responsibility of the Contractor to validate the information security standards and controls of any subcontracted organization or individual in accordance with the same requirements extended to the Contractor by NJ TRANSIT.

18. Upon request, the Contractor shall provide to NJ TRANSIT verification, to the extent required by the NJ TRANSIT Chief Information Security Officer or his/her delegate, that validation of security standards and controls for subcontracted party(s) has taken place.

19. The Contractor shall immediately notify the NJ TRANSIT Chief Information Security Officer of any information security incident that may affect NJ TRANSIT information and systems.

20. The Contractor shall maintain an incident response plan that specifically states this requirement and shall provide this incident response plan to NJ TRANSIT for review, subject to the Contractor's standard document review process (i.e. on site, closed-door, mutual NDA, etc.).

21. Contractor shall conduct background checks for each consultant assigned to the project. When requested, Contractor will provide documented evidence of background checks for each consultant assigned to the project.

22. Contractor shall surface issues, suggest options, and make recommendations to NJ TRANSIT in regard to information security based on the classification of data as described in the NJ TRANSIT's

Data Classification Policy. This includes all material issues identified, regardless of infrastructure ownership.

23. Contractor shall identify and provide contact information for the person who has overall responsibility for information security within its organization. When requested, Contractor agrees to provide a copy of its information security policies.

24. A Contractor may not export NJ TRANSIT data classified as “CONFIDENTIAL” or “RESTRICTED” outside the United States except with the expressed written permission of the NJ TRANSIT Chief Information Security Officer. “CONFIDENTIAL” and “RESTRICTED” shall have the meaning ascribed to in the NJ TRANSIT’s Data Classification Policy.

25. Contractor must obtain written permission from NJ TRANSIT for each method of remote access it wishes to use to access NJ TRANSIT data.

26. Should Contractor learn or suspect that there has been a breach of this policy, it shall immediately notify the NJ TRANSIT’s IT Cyber Security Department.

27. In the case of a breach to the contractor’s computing environment, NJ TRANSIT may impose additional and more stringent, information security requirements than those in this policy, as applicable. Contractor shall review the new requirements and propose short-term and long-term compensating controls to mitigate risk and apply best efforts to remedy security gaps. NJ TRANSIT and the Contractor shall work together to determine a mutually agreeable cost proposal.

28. The Contractor’s obligations for record retention under this policy shall survive the termination or expiration of the Agreement for 7 Years.

Integration and IT Architecture

29. NJ TRANSIT uses a wide range of integrated hardware and software to support its operations. The standards below balance the need for flexibility with the equally important need to establish an infrastructure that can last into the future to the maximum extent practical. Applicable IT standards currently in use at NJ TRANSIT are summarized below. Contractors must demonstrate their solution will perform acceptably within its technology environment(s) and networks.

30. NJ TRANSIT is taking a proactive approach when it comes to securing our computers from malware and any other type of misuse of the NJ TRANSIT’s information assets. It is required that all new applications satisfy the following criteria for consideration to use at NJ TRANSIT:

    30.1 During the Contractor’s SDLC and prior to implementation on an NJ TRANSIT network, Contractor shall apply all critical software patches before a computer or any other device is connected to the NJ TRANSIT network.

    30.2 All computers shall run appropriate anti-malware software and patch management software that is approved by NJ TRANSIT.

30.3 Only authorized users shall have local administrative access to infrastructure and computers.

30.4 Contractors shall ensure that any software that runs on NJ TRANSIT client computers can be installed and run where the computers are "locked down". NJ TRANSIT users do not have the ability to write to the computer's hard disk or registry with the exception of their own profile (i.e. "my documents" section and HKEY_CURRENT_USER registry keys).

30.5 "Critical" patches shall be applied to the product development environment according to the Contractor's CSP. The contractor is required to test patches prior to implementation and testing must be completed within an approved implementation window.

30.6 Contractor shall ensure that any server or client-based application that is intended to be run in an unattended mode must be installed and run as a system service so that a user does not need to be logged on to the system for the application to function.

Environment Standards and Requirements

The contractor shall follow the following standards. Exceptions may be granted, in writing, on a case by case basis by NJ TRANSIT's Chief Information Security Officer.

Operating Systems

31. The version of any operating system selected for use must have a minimum of 5 years of vendor support available after the in-service date.

Network Protocols

32. The network protocol used shall be TCP/IP.
33. TLS protocols used must not be deprecated versions.

Databases

34. The version of any database selected must be current and have a minimum of 5 years of vendor support available after the in-service date.

Database Security Requirements (<u>where applicable</u>)

35. Contractor access to data must be documented and periodically reviewed.
36. The Database schema owner account cannot be used to run the application. A separate user account must be created for application access.

Configuration Standards

37. All operating systems (OS), hardware, firmware, software must adhere to configuration best practices as defined by the Center for Internet Security (CIS) or the vendor supplying the OS, hardware, firmware, or software.
38. The Contractor must supply documentation of configurations used.

Anti-Malware

39. NJ TRANSIT requires anti-malware protection for its computing environments. The anti-malware solution must be approved by the Chief Information Security Officer.

Vulnerability and Patch Management

40. Contractor must provide a documented vulnerability management plan. The plan must include the items listed below. All exceptions must be approved by the Chief Information Security Officer.

    40.1 Goods, services, and work product provided by the Contractor must be fully patched prior to delivery.

    40.2 Contractor must have a process capable of identifying new vulnerabilities.

    40.3 Contractor is required to utilize a vulnerability management tool to identify vulnerabilities and manage patching of goods, services and work products provided to NJ TRANSIT.

    40.4 The vendor is responsible to perform and review frequent vulnerability scans to identify all potential vulnerabilities for the goods, services, and work products provided to NJ TRANSIT.

    40.5 Vendor must identify and notify NJ TRANSIT when “Zero Day” exploits are found that affect their systems. Vendor must review and determine appropriate steps taken to mitigate or address “Zero Day” exploit risk within 24 hours. Patching, if appropriate, must be completed within five (5) business days.

    40.6 For critical vulnerabilities that affect their systems, Contractor must assess and develop an action plan to mitigate/address risk and notify NJ TRANSIT within (5) business days.

Logging and Auditing

41. Logging capabilities must be supported to cover the following events, at a minimum:
    41.1 Successful and unsuccessful authentication and access attempts
    41.2 Account changes
    41.3 Privileged use
    41.4 Application / Service / System start-up and shutdown
    41.5 Application / Service / System failures
    41.6 Configuration changes to the application, service, system, or database used
42. Log files must be kept for eighteen (18) months.

Firewall

43. Where firewalls are included as part of the system the following applies:
    43.1 Software shall be configurable to allow for a proxy.
    43.2 Software that must communicate via the Internet to another site shall allow for proxy authentication and SSL inspection.
    43.3 Software shall not use client-side encryption other than SSL without prior approval of the Chief Information Security Officer or his/her designee.

43.4 Communications not using 'well-known ports' shall list such requirements prominently in the proposal.

Application Security

44. Contractor shall ensure the Contractor Application is compatible with Microsoft's Active Directory Architecture.
45. NJ Transit requires that each application be able to identify a user as pass-through (no need to re-enter password) or as re-authenticate (must re-enter password) before access to the application is granted.
46. Any application not compatible with Microsoft Active Directory architecture must be approved by NJ TRANSIT's Chief Information Officer.
47. The version of any application software selected must be current and have a minimum of 5 years of vendor support available after the in-service date.

Time Source

48. All computers shall be automatically and continuously synchronized to standard New Jersey Transit time sources.

Desktop Software Standards

49. The application should be capable of being installed to any drive or directory.
50. Software distributions must be packaged as an Installer distribution in MSI 3.1 format (or higher). The MSI must be able to be installed as a parameter to MSIEXEC.EXE and must not require the use of an external "setup.exe" executable. Alternate installers or exceptions may be approved by NJ TRANSIT at the Contractor's request.
51. The package should default to a directory under "C:\Program Files" unless otherwise chosen during installation.

Escrow

52. If NJ TRANSIT is not provided with a copy of the product's source code, a copy of the source code shall be delivered on a mutually agreed upon electronic or disk media to a vault storage facility, identified by NJ TRANSIT. The source code shall be independently logged, verified at the facility, and held in escrow to ensure that NJ TRANSIT has appropriate backup and reconstruction capability.

Additional Cyber Security Requirements

53. Any additional cyber security requirements specific to the goods, services, and work products provided to NJ TRANSIT under this Agreement are further defined in Addendum A: Additional Cyber Security Requirements if required.