Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

Company Name: MVC LOAP Account Number (if renewing):

Name of Company Representative: Title of Company Representative:

Phone Number: Email Address:

Date: Approximate Number of Company Employees:

The New Jersey Motor Vehicle Commission (MVC) requires that customers of the Limited Online Access Program (LOAP) perform due diligence in their protection of any information and data obtained through the program. The protection of this information and data is of the utmost importance for the MVC. The sensitivity of this data and the increase of identity theft requires that MVC partner with you to ensure that we both meet our obligations under the Federal and New Jersey Drivers' Privacy Protection Act, 18 U.S.C. 2721 to 2725, and N.J.S.A. 39:2-3.3 to 3.6 (Federal DPPA and New Jersey DPPA) and that your technology environment meets both Federal Information Security Management Act, 44 U.S.C. 3551, et seq. (FISMA) and the National Institute of Standards and Technology (NIST) standards. The terms and conditions related to protection of this information and data can be found within the LOAP agreement. Applicants for the LOAP program must be able to demonstrate their ability to comply with these terms and conditions.

Definitions

The Federal Drivers' Privacy Protection Act (federal DPPA) is a law that limit the occasions when state departments of motor vehicles and authorized recipients may disclose to the public personal information contained in a person's motor vehicle record, which includes a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles. Many states have enacted similar legislation further regulating this data. (18 U.S.C. 2721, *et seq.)*

The New Jersey Drivers' Privacy Protection Act (New Jersey DPPA) is a State law that limits the occasions when the MVC and authorized recipients may disclose to the public personal information contained in a person's motor vehicle record, which includes a motor vehicle operator's permit, motor vehicle title, motor vehicle registration, or identification card issues by the MVC. (N.J.S.A. 39:2-3.3, *et seq*.)

Personal Information (PI) means information that identifies an individual, including an individual's photograph; social security number; driver identification number; name; address other than the five-digit zip code; telephone number; and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver's status. (N.J.S.A.39:2-3.3)

Personally Identifiable Information (PII) means any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Executive Branch of New Jersey State Government Statewide Information Security Manual, pg. 48 (SISM)).

Scope of the questionnaire

All MVC Personal Information and Personally Identifiable Information (see below) data held in electronic format or contained within a structured manual filing system must be secured. In particular, but not exclusively, this questionnaire will cover PI and PII data held in the following systems and formats:

- Personal Computers
- Databases
- Servers
- Virtual Machines
- Cloud Services
- Document management systems (including documents stored in standard directory structures)
- Individual computer files where appropriate, e.g., spreadsheets and other such analysis tools, word-processed lists
- Structured e-mail directories
- Structured manual filing systems that can be referenced by individual, e.g., student files, staff files, survey data forms, examination scripts, holiday charts/lists, directories, publication lists
- Web-pages
- Microfiche
- CD's
- Thumb drives or memory sticks

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

- Any other storage devices not listed here

Please note that in evaluating questionnaire it may be necessary to meet with staff within your organization to ensure that PI and PII is being handled uniformly and according to the aforementioned standards.

Please complete this questionnaire and submit it with your application. All parts must be completed. Do not leave blanks. If something is not applicable, please indicate this on the questionnaire and explain why. If more space is needed to provide the information requested, indicate next to the question and attach additional pages. All pages of this questionnaire must be returned. If you have any questions or wish to discuss any of the requirements, please contact the MVC Information Security Office at mvcinfosec@mvc.nj.gov

Please select how your organization accesses and stores MVC data and information (select all that apply) and then complete the applicable sections:

☐ Viewing on Screen	Complete Section 1
☐ Viewing and Printing	Complete Sections 1 & 2
☐ Store Electronically on local machine (PC, Laptop)	Complete all Sections
☐ Store electronically on external media (hard drive, flash drive, DVD/CD)	Complete all Sections
☐ Store electronically in an application (website, mobile app, etc.)	Complete all Sections
☐ Transmitted Electronically (to server, another entity, email, etc.)	Complete all Sections

Section 1

User Access:

1. **If you are renewing your application**, provide a list of the users in your organization who have access or who will have access to the MVC's LOAP system. Please be advised that each user **MUST** have their own logon ID (If necessary, attach a separate sheet of paper).
   List ALL users who will have (current and future) access to the MVC LOAP System.

Name:	E-Mail Address:	Logon ID:

2. Does your organization implement processes to ensure all personnel have the appropriate background, skills, and training to perform their job responsibilities in a competent, professional, and secure manner? Workforce security controls include, but are not limited to:
   Have you executed pre-employment background checks for skilled employees and once hired, advised them of general employment policies and practices, job responsibilities, computer data security and awareness?

   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 organization information assets;
   c. Rules of behavior are established, and procedures are implemented to ensure personnel are aware of and understand usage policies applicable to the organization's information and information systems;
   d. Access reviews are conducted upon personnel transfers and promotions to ensure access levels are appropriate;
   e. Disabling system access for terminated personnel and collecting 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 organizational information assets and their responsibility to immediately report any suspected information security incidents.

   ☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

3. Please describe the screening and background checks you conduct for your workforce, (employees, contractors, and third parties), if any, that have access to the MVC's LOAP system (e.g., CJI, FTI, PCI, etc.).
What are the types of background checks done for the employees using the MVC LOAP System?

4. Are all personnel required to sign an Acceptable Use Policy (AUP)? If you answered yes, please submit a copy of the AUP. If no, please explain.
Acceptable Use Policy is document signed by employees stipulating constraints and practices they must agree to for access to the business network or the Internet.

5. Briefly describe the procedures your organization follows to govern changes in employment (transfers, promotions, etc.) and/or termination of staff.
How is the computer access removed once an employee has moved on?

6. Please detail your organization's disciplinary policy for personnel who have violated security policies and procedures.
Is an employee terminated if they violate computer access policies or data confidentially, explain?

7. Does your organization provide information security awareness and training to ensure employees 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 information from a loss of confidentiality, integrity, availability, and privacy? Security awareness and training includes, but is not limited to:
Do your employees understand the role they play in helping to combat information security breaches, the security risks associated with their actions and to identify cyber-attacks they may encounter via email and the web?

   a. Employees and contractors are provided with security awareness training upon hire and at least annually, thereafter;
   b. Security awareness training records are maintained as part of the employee's personnel record;
   c. Role-based security training is provided to individuals 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.

☐ Yes ☐ No

8. Describe the security awareness and training program you provide to employees and contractors to ensure they are aware of information security risks and threats, understand their responsibilities, and are aware of the statutory and policy requirements. Is the training mandatory? How is training by personnel documented and tracked? How often is security awareness training conducted?
This is the process of teaching your employees computer and information security best practices, as well as educating them on the various security threats we face today.

9. Does your organization's training include the proper handling of MVC PI and PII data?
The MVC data you have access to when viewed, printed, or saved, it is confidential and only available to those authorized to the LOAP on-line system. This data should always be locked and always secured.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

Section 2

10. Does your organization establish requirements for the identification, assessment, and treatment of information security risks to organization operations, information, and/or information systems? Risk management includes, but is not limited to:
If you have done any of the following vulnerability practices noted below, answer Yes

    a. Categorizing systems and information based on their criticality and sensitivity;

    b. Ensuring risks are identified, documented, and assigned to appropriate personnel for assessment and treatment;

    c. Ensuring risk assessments are 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. Mitigating risks to an acceptable level and prioritizing remediation actions based on risk criteria and establishing timelines for remediation. Risk treatment may also include the acceptance or transfer of risk.

☐ Yes ☐ No

11. Describe the risk management processes you employ that account for the identification, assessment, and treatment of risks that can adversely impact the confidentiality, integrity, and availability of the product/system/application/service. How often are these risk management processes performed?
Do you have a current listing of all your computers and servers that have or use MVC PII data and how often is this list reviewed?

12. Describe how risks and risk mitigation efforts are evaluated and prioritized. Include details on how you document and verify the results of these risk mitigation processes?
The actions to reduce vulnerability to threats and hazards, countermeasures and project deployment planning are a key outcome of the planning process.

13. What physical and environmental protection measures does your organization have in place that limits access to the systems, equipment, data, and respective operating environments, to only authorized individuals? Physical and environmental controls include, but are not limited to, physical access controls, security monitoring and auditing of physical access, visitor controls, water damage protection, fire protection, etc.
Do you have any of the following: visitor logs, security cameras, locked doors, locked filing cabinets, password protected computers, smoke alarms where your computers, servers and files are located that display, store or transmit MVC PII Data?

14. Has your organization established appropriate processes and safeguards necessary to protect the PII that your organization collects, stores, processes, uses, and transmits from the MVC? Privacy controls and processes include, but are not limited to:
Is the Is MVC PII data deleted and/or shredded when no longer a needed and protected from unauthorized users at rest (in a locked file or encrypted on a computer or server) and in transit (when emailing).

    a. Ensuring only the minimum amount of PII necessary to carry out the business function, and in accordance with applicable laws and regulations, is collected and stored;

    b. Safeguarding PII through the implementation of administrative, physical, and technical controls (e.g., access controls, encryption, and tokenization, etc.); and

    c. Securely deleting PII when no longer necessary for business or legal purposes.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

15. Describe your privacy program and detail how it maintains current with evolving applicable privacy requirements.
How often this document is updated describing the types of personal data you process, its origin, how long it is kept and if transferring to third parties.

16. Has your organization established controls to ensure data and information, in all forms and mediums, are protected throughout their lifecycles based on sensitivity, value, and criticality, and the impact that a loss of confidentiality, integrity, availability, and privacy would have on your organization, business partners, or individuals? Media protections include, but are not limited to:
Does your organization have a records retention policy to delete and/or shred employee MVC PII data when no longer a necessity or it meets the timeline for its lifecycle and integrity?

    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.

☐ Yes ☐ No

17. How long does your organization retain MVC data and information and where is it stored?
How long do you keep the printed MVC data and where is located or if electronically saved to pc or server, how long is it kept?

18. Is MVC data and information physically co-mingled with other data?
Do you keep MVC printed data in a locked cabinet with other employee records? If electronically stored on a pc or server, are you backing up all of your data together or is MVC data backed up separately?

Section 3

19. What Operating System (OS) version(s) are your servers, laptops, and desktop computers utilizing? If you are not running the latest version(s), do you have plans and a timetable for upgrade? If yes, what are your plans and timetable for upgrades?
Popular Operating Systems are Microsoft Windows and are Apple macOS. For Windows, next to the Start or Windows button (usually in the lower-left corner of your computer screen) type ABOUT in the white search box. The resulting screen shows the edition of Windows.

20. What anti-virus and related software are you currently utilizing and what version(s)? If you are not running the latest version(s), do you have plans and a timetable for upgrade? If yes, what are your plans and timetable for upgrade?
An antivirus product is a program designed to detect and remove viruses and other kinds of malicious software from your computer or laptop.

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

21. When accessing or manipulating MVC data, is your organization logging the anti-virus, anti-spyware, or anti-malware events from your servers, laptops, desktop computer, or any other devices?
Event logs are special files that record significant events on your computer, such as when a user logs on to the computer or when a program encounters an error.

22. Has your organization established and maintained a framework to provide assurance that information security strategies are aligned with and support business objectives, are consistent with applicable laws and regulations through adherence to policies and internal controls, and provide assignment of responsibility, all in an effort to manage risk? Information security program management includes, but is not limited to, the following:
Dose your organization protect the information and systems that support the operations and protect from unauthorized access and disclosure, assuring the reliability and accuracy and ensuring a timely reliable access and use of information?

    a. Establishment of a management structure and responsibility for information security;
    b. Creation, maintenance, and communication of information security policies, standards, procedures, and guidelines to include the control areas listed 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 organization's information security program.

☐ Yes ☐ No

23. Does your organization align your information security program(s) with any of the following industry standard frameworks such as the NIST CSF, ISO 27001, CIS Top 20, CoBIT? If yes, please list which framework(s) you employ.
NIST has become the gold standard for assessing cybersecurity maturity, identifying security gaps, and meeting cybersecurity regulations. Its industry framework consists of five concurrent and continuous Functions, Identify, Protect, Detect, Respond and Recover.

24. Does your organization periodically assess security controls within your information system(s)? If so, please describe the process that your organization follows to review and update your security controls. ***This is a process of exanimating, reviewing, and testing information system security prior to or after a system is in operation. Some methods are Vulnerability Assessment, Penetration Testing, Log Reviews, Synthetic Transactions, Code Review and Testing, Misuse Case Testing, Test Coverage Analysis, and Interface Testing.***

25. If your organization employs an Exception Management Policy, please document the processes for the submission, review, documentation, and the application of exceptions to compliance with established information security policies and practices.
This is when a department or school is not able to meet the policies and standards will submit a policy exception request form to explain why compliance is not possible, systems(s) that will be impacted, information and system classification, end users, impact, duration for the exception, suggestions of compensating controls.

26. Has your organization developed, implemented, and governed processes to ensure compliance with all applicable statutory, regulatory, contractual, and internal policy obligations? Ensuring compliance includes, but is not limited to:
If you have done any of the following vulnerability practices noted below, answer Yes

    a. Statutory, Regulatory, and Contractual Compliance;
    b. Security controls oversight; and
    c. Periodically conducting security assessments.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

27. Does your organization conduct any third-party security audits to ensure compliance with applicable laws, regulations, and contractual requirements? If so, please state the type of audit conducted and last audit date (e.g., CJJS, FedRAMP, FISMA, IRS-1075, PCI-DSS, Social Security Administration, SOC2).
A third-party audit is performed by an audit organization independent of the customer-supplier relationship and is free of any conflict of interest. Independence of the audit organization is a key component of a third-party audit.

28. Specify all compliance frameworks and standards your organization follows (e.g., GDPR, COBIT, ISO, etc.).
Compliance and regulatory frameworks are sets of guidelines and best practices to improve processes, strengthen security, and achieve other business objectives.

29. Has your organization implemented 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 include, but are not limited to:
Password protection, security cameras, locked doors and creating a network security key, changing the advanced settings, and turning on Windows firewall protection are types of controls.

    a. Information technology asset identification and inventory;

    b. Assigning custodianship of assets; and

    c. Restricting the use of non-authorized devices.

☐ Yes ☐ No

30. Has your organization established a formalized mechanism 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, but is not limited to:
If you have done any of the following vulnerability practices noted below, answer Yes

    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; and

    b. Subscribing to and receiving relevant threat intelligence information from the US CERT, the organization's vendors, and other sources as appropriate.

☐ Yes ☐ No

31. List and describe the threat intelligence sources you subscribe to or follow in order to keep abreast of potential security vulnerabilities and threats.
These are the sources of strategic, operational, and tactical information resources you use to help you make better decisions about how to defend yourself and your business from cyber-based threats.

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

32. Has your organization established security requirements and ensured appropriate mechanisms are provided for the control, administration, and tracking of access to, and the use of, the organization's information systems? Access management includes, but is not limited to:
If you have done any of the following vulnerability practices noted below, answer Yes

    a. Ensuring 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. Implementing account management processes for registration, updates, changes, and de- provisioning of system access;

    c. Provisioning access according to an individual's role and business requirements for such access;

    d. Implementing the concept of segregation of duties by disseminating tasks and associated privileges for specific sensitive duties among multiple people;

    e. 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;

    f. Implementing multi-factor authentication (MFA) requirements for access to sensitive and critical systems, and for remote access to the organization's systems and information; and

    g. Conducting periodic reviews of access authorizations and controls.

    ☐ Yes ☐ No

33. Describe your organization's processes and methods utilized for granting access, reviewing access, and documenting the review. Do you centrally manage access throughout the organization? Explain in detail.
A user access review is part of the user account management and access control process, which involves a periodic review of access rights for all of an organization's employees and vendors. A user access review usually includes re-evaluation of User roles, Access rights and privileges, Credentials provided to users.

34. Detail your password and authentication policy and standards. Include minimum length, lockout, complexity, timeout period, password history, etc. How are these managed and enforced?
A strong password must be at least 8 characters long. It should not contain any of your personal information — specifically, your real name, username, or your company name. It must be very unique from your previously used passwords and should be regularly changed.

35. Is the MVC data encrypted at rest and at transmission? If so, please detail the mechanisms used to secure MVC data at rest, data in transit, and data in use.
Data protection in transit is the protection of this data while it's traveling from network to network or being transferred from a local storage device to a cloud storage device or email. Data at rest is data that is not actively moving from device to device or network to network such as printed data, data stored on a hard drive, laptop, flash drive, or archived/stored, in some other way.

36. Describe the process of controlling and monitoring the use of privileged and administrative accounts within your organization. Is Multi-Factor Authentication (MFA) required for privileged access? Do end-users have local administrator access?
Multi-factor Authentication (MFA) is an authentication method that requires the employee to provide two or more verification factors to gain access to a resource such as an application, online account, or a VPN. Administrator Access is defined as a level of access above that of a normal employee.

37. If employees and/or contractors are provided with remote access to your organization's internal network, please describe the mechanisms used for authentication and authorization. Detail the use of MFA for remote access, if applicable.
This could be your IT department/contractor or employees who can access a work computer desktop or server and its files from a remote location. Describe the software/process used to do this.

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

38. Has your organization employed security engineering and architecture principles for all information technology assets, such that they incorporate industry recognized leading security practices and address applicable statutory and regulatory obligations? Applying security engineering and architecture principles include, but are not limited to, the following:
If you have done any of the following vulnerability practices noted below, answer Yes

    a. Implementing configuration standards that are consistent with industry-accepted system hardening standards and addressing 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 across the organization.

    ☐ Yes ☐ No

39. Has your organization ensured 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 includes, but is not limited to:
Minimum security baselines are standards for all systems in the network, ensuring that they meet a set of minimum requirements to avoid risking the entire network.

    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.

    ☐ Yes ☐ No

40. Describe the processes employed to establish and maintain baseline security configuration settings across your organization. Industry standard configuration and hardening standards include, but are not limited to, CIS Benchmarks, DISA STIGs, and component vendor security configuration guides.
The Center for Internet Security (CIS), provide prescriptive guidance for establishing a secure baseline configuration for assets. The CIS Benchmarks are the only consensus-based configuration best practice guidelines developed by a global community of cybersecurity professionals and experts from all walks of life and are accepted by governments, businesses, industries, and academia.

41. Describe the processes and protective technologies employed to verify these security configuration settings are maintained and to detect any attempts to adversely impact the confidentiality, integrity, and availability of components or data in your organization. Protective technologies include, but are not limited to, firewalls, host and network intrusion detection/protection systems, file integrity monitoring, and anti-malware software
This could be an antivirus software loaded on a pc, a firewall to prevent unauthorized access into or out of a computer network or an IT security process and technology that tests and checks operating system (OS), database, and application software files to determine whether or not they have been tampered with or corrupted.

42. Describe cryptographic standards and technologies, if any, employed to protect sensitive MVC data and information. Include details on the encryption and or hashing algorithms used, key management processes, use of hardware or software key storage, key fragmentation, etc.
Cryptographic mechanisms are required to secure data at rest or in transit. These techniques provide several security requirements, such as confidentiality, data integrity, entity authentication, message authentication, key management, non-repudiation, trustworthy data platforms, and digital signatures.

43. Has your organization ensured that endpoint devices are properly configured, and measures are implemented to protect the organization's information and information systems from a loss of confidentiality, integrity, and availability? Endpoint security includes, but is not limited to:
Endpoint security or endpoint protection is an approach to the protection of computer networks that are remotely bridged to client devices.

    a. Maintaining an accurate and updated inventory of endpoint devices;
    b. Applying security categorizations and implementing commensurate 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.

☐ Yes ☐ No

44. Describe the standard employee issued device security configuration/features (Login Password, anti-malware, full disk encryption, administrative privileges, firewalls, auto-lock, etc.).
Do employees have administrative privileges and what is on the computers when delivered and configured?

45. Are all endpoints in or with access to the production environment centrally managed? Explain.
Microsoft Endpoint Configuration Manager (also known as ConfigMgr or MECM), formerly System Center Configuration Manager (SCCM) and Systems Management Server (SMS) is a systems management software product developed by Microsoft for managing large groups of computers. Are your Windows endpoints managed with SCCM.

46. Describe how you limit data exfiltration of sensitive data from endpoints in or with access to the production environment.
Best practice, consider disabling all unauthorized communication channels, ports, and protocols by default, then enabling them on an as-needed basis. This approach offers a stronger data security policy than one where all entryways are enabled by default.

47. Has your organization established controls required to ensure change is managed effectively? Organizations must ensure changes are appropriately tested, validated, and documented before implementing any change on a production network. Change management provides the organization 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 include, but are not limited to, the following:
Change requests reviewing, planning, assessing, and implementing a request for changes in an effective manner.

    a. Notifying all stakeholders of changes;
    b. Conducting a security impact analysis for changes; and
    c. Verifying security functionality after the changes have been made.

☐ Yes ☐ No

48. Describe the change control process as it relates to patches, hot-fixes, upgrades, and configuration changes within your organization. Include information on review of proposed changes. Include information on timelines used for testing, implementation, and emergency change control.
Are critical updates applied after testing and other server patches within a particular time frame and notifications in advance of any outages?

49. Has your organization implemented 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 includes, but is not limited to:
Perform scheduled operational and strategic management of hardware and software.

    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 the organization's information technology assets.

☐ Yes ☐ No

50. Has your organization implemented continuous monitoring practices to establish and maintain situational awareness regarding potential threats to the confidentiality, integrity, availability, privacy, and safety of the organization's information and information systems through timely collection and review of security-related event logs? Continuous monitoring practices include, but are not limited to:
Performing ongoing security assessments and monitoring whether the set of deployed security controls remains effective in light of new exploits and attacks and planned and unplanned changes that occur in the system and its environment over time.

    a. Centralizing the collection and monitoring of event logs;
    b. Ensuring the content of audit records includes all relevant security event information;
    c. Protection of audit records from tampering; and
    d. Detecting, investigating, and responding to incidents discovered through monitoring.

☐ Yes ☐ No

51. Describe the processes and technologies used for monitoring, alerting on, and logging of application, system, network, and security events. Include information on retention of logs and how they are reviewed.
How often are your event logs reviewed for incident analysis and actionable information concluded for future prevention?

52. Has your organization implemented 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 include, but are not limited to:
Companies should be wary of third-party risk and have management processes in place for not only vendors, contractors, customers, and joint ventures, but also counterparties and fourth parties.

    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 organization's systems and sensitive information;

    c. Third-Party interconnection security; and

    d. Independent testing and security assessments of supplier technologies and supplier organizations.

☐ Yes ☐ No

53. Describe the processes utilized to validate third-party service providers' compliance with applicable laws, regulations, and contractual requirements.
Is there a report or logs generated and monitoring when access is obtained?

54. Has your organization developed, implemented, tested, and maintained contingency plans to ensure continuity of operations for all information systems that deliver or support essential or critical business functions on behalf of the organization? Contingency planning includes, but is not limited to:
Effective contingency planning, execution, and testing are essential to mitigate the risk of system and service unavailability.

    a. Backup and recovery strategies.

    b. Continuity of operations plans.

    c. Disaster recovery plans; and

    d. Crisis management plans.

☐ Yes ☐ No

55. Describe the processes and plans that are implemented to ensure continuity of operations for your organization.
Are systems being backed up with test restores occurring regularly?

56. Describe the data and system backup/recovery processes employed and how the security categorization of the information is maintained by the backup media. How often are backups tested to verify media reliability and information integrity? What are the recover point and recovery time objectives?
How often are backups executed and on what media or cloud and do you have mirroring? Is there any media reliability testing?

57. As applicable, if an alternate site(s) has been established for storage, processing, and communication functions as a part of the organization's contingency plan, describe the processes and timelines for falling over. Is the alternate site considered Hot, Warm, or Cold? Explain. How often are fall-over processes tested and how are the resulted documented and reviewed?
A Hot Site is available immediately, Warm Site is days or hours, and Cold Site is weeks for a fall over and has this fall over been tested?

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

58. Has your organization maintained an information security incident response capability that includes adequate preparation, detection, analysis, containment, recovery, and reporting activities. Information security incident response activities include the following:

    a. Information security incident reporting awareness;

    b. Incident response planning and handling;

    c. Establishment of an incident response team;

    d. Contracts with external incident response services specialists; and

    e. Contacts with law enforcement cybersecurity units.

☐ Yes ☐ No

59. Describe how your organization's incident response procedure is tested and how often tests are conducted.
If data needed to be restored, what is the procedure and has this procedure ever been utilized.

60. Describe in detail any breaches of information security your organization experienced over the past five years. Describe how affected customers were notified by your organization, the timeframe of such notifications, and steps taken by your organization to prevent the breach from recurring.
If no breaches in the past five years state that, otherwise; describe.

61. Does your organization currently have cyber liability insurance coverage? If so, please provide a declarations page for your policy.
Cyber liability insurance is an insurance policy that provides businesses with a combination of coverage options to help protect the company from data breaches and other cyber security issues.

62. Has your organization implemented processes that classify information and categorize information systems throughout their lifecycles according to their sensitivity and criticality, along with the risks and impact should there be a loss of confidentiality, integrity, availability, or privacy? Information classification and system categorization includes labeling and handling requirements. Security Categorization controls include, but are not limited to, the following:
If you have done any of the following vulnerability practices noted below, answer Yes

    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.

☐ Yes ☐ No

63. Has your organization implemented 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 included here in this document, including, but not limited to:
If you have done any of the following vulnerability practices noted below, answer Yes

    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 organization'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.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

64. As applicable, list and describe and ICS/SCADA/OT systems used across your organization and detail how those systems are secured physically, administratively, and technically.
OT/ICS/SCADA - Operational Technology, Industrial Control Systems and Supervisory Control and Data Acquisition Systems. ICS are command and control networks and systems designed to support industrial processes. The largest subgroup of ICS is SCADA (Supervisory Control and Data Acquisition) systems.

65. Has your organization implemented 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 security includes, but is not limited to, the following:

If you have done any of the following vulnerability practices noted below, answer Yes

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 organization's networks; and
e. Ensuring least privilege and strong authentication controls are implemented.

☐ Yes ☐ No

66. As applicable, list and describe any IoT devices used across your organization and detail how those devices are secured physically, administratively, and technically. Include information on network segmentation, access and authentication, and security updates.
Are all IOT devices MAC authorized and have an IP address and all remote devices connected to VPN controlled with NAC and MFA to reduce risk

67. Has your organization established administrative, technical, and physical security controls required to effectively manage the risks introduced by mobile devices used for organizational business purposes? Mobile device security includes, but is not limited to, the following:
If you have done any of the following vulnerability practices noted below, answer Yes

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 of approved applications that can be used; and
h. Training of mobile device users regarding security and safety.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

68. Does your organization allow for BYOD devices to connect to your internal network? If so, how are BYOD managed so they do not introduce additional risks?
BYOD is employees accessing the work data and systems using personal mobile devices such as smartphones, tablets, and laptops. Applying security policies, distribute enterprise approved app and share the required corporate content to bring devices under management to mitigate risks.

69. Has your organization implemented defense-in-depth and least privilege strategies for securing the information technology networks that they operate? To ensure information technology resources are available to authorized network clients and protected from unauthorized access, organizations must:

If you have done any of the following vulnerability practices noted below, answer Yes

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 organization's information systems (e.g., network segmentation, network intrusion detection and prevention systems, wireless restrictions, etc.).

☐ Yes ☐ No

70. Has your organization established 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 includes, but is not limited to, ensuring the following:

If you have done any of the following vulnerability practices noted below, answer Yes.

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 interfaces are conducted in accordance with mutually agreed-upon service, security, and capacity-level expectations;

c. Security roles and responsibilities for the organization and the cloud provider are delineated and documented; and

d. Controls necessary to protect sensitive data in public cloud environments are implemented.

☐ Yes ☐ No

71. Has your organization implemented 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 include, but are not limited to, the following:

If you have done any of the following vulnerability practices noted below, answer Yes.

a. Prioritizing vulnerability scanning and remediation activities based on the criticality and security categorization of the organization's 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 conduct independent vulnerability scanning, penetration testing, and red-team exercises.

☐ Yes ☐ No

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

NEW JERSEY MOTOR VEHICLE COMMISSION TECHNOLOGY QUESTIONNAIRE

72. Describe your network vulnerability scanning and penetration testing process. Who conducts your network penetration testing and vulnerability scan? Are these vulnerability scans and penetration tests both external and internal? How often are vulnerability scans and penetration tests conducted?
Vulnerability scanning is an inspection of the potential points of exploit on a computer or network to identify security holes. A vulnerability scan detects and classifies system weaknesses in computers, networks and communications equipment and predicts the effectiveness of countermeasures. An external vulnerability scan is a scan that is conducted outside of the network you're testing. These scans target external IP addresses throughout your network, scanning perimeter defenses like websites, web applications, and network firewalls for weaknesses.

73. Describe how patches and vulnerability remediation processes are prioritized. How do you document and verify the results of these remediation efforts?
Is checking and applying manufacturer updates and patches done on a regular basis along with reviewing recommended remediations causes?

74. As applicable, please provide details on the most recent Application Code Review or Penetration Testing Reports carried out by independent third parties.
Application Security Code Review is the manual review of source code with the developers to identify source code-level issues that may enable an attacker to compromise an application, system, or business functionality.

If you are either printing, storing, or transmitting data electronically:

☐ Copy of your Privacy Policy

New Jersey Motor Vehicle Commission

Mail to:
Business & Government Services
P.O. Box 122
Trenton, NJ 08666-0122
Phone: 609-292-4572

☐ Other relevant documentation, reports, information (please provide details below).

Only if you are storing or transmitting data electronically:

☐ Independent information security audits and/or certifications (e.g., PCI-DSS, SOC2 Type II, ISO27001, FEDRAMP, FISMA certification).

☐ As applicable, if the service/application you are intending to provide to the State of New Jersey relies on other vendors or Cloud Service Providers (CSP) (e.g., Amazon, Salesforce, Microsoft, Google, etc.), please submit relevant security profiles/certifications for the vendors and/or CSPs being utilized.

☐ Copy of your organization's written information security policies and standards

☐ Other relevant documentation, reports, information (please provide details below).

_____
Company Representative Name

_____
Company Representative Signature

_____
Date

Please submit the following supporting documentation with this questionnaire according to LOAP data use: