

Vendor Security & Compliance Questionnaire

- Outsource

Version 1.0

# Company Information

Name of Company: Click here to enter text.

Company Website: Click here to enter text.

Contact Person Completing the Questionnaire: Click here to enter text.

Email Address: Click here to enter text.

Phone Number: Click here to enter text.

Date of Completed Questionnaire: Click here to enter text.

# Questionnaire Completion Instructions

1. Select the appropriate answer in each Response section.
2. Provide additional details in the “Describe” column to support every answer.
3. Include attachments as necessary to support the given information.

| **Question** | **Requirement** | **Response** | **Describe** |
| --- | --- | --- | --- |
| 1.  | An individual has been designated as being responsible for security within the organization. | Yes [x] No [x] n/a [ ]  |  Click here to enter text. |
| 2.  | An information security policy, based on industry acceptable standards and frameworks, is in place, has been approved by management and has been communicated to employees, contractors and individuals working on behalf of the organization. | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 3.  | Security roles and responsibilities of employees, contractors and individuals working on behalf of the organization are defined and documented in accordance with the organization’s information security policy. | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 4.  | An information security awareness and training program has been established and provides general awareness and role specific (e.g., secure coding, CJIS, etc.) security training to all employees. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 5.  | Background screenings of employees, contractors and individuals working on behalf of the organization are performed to include criminal, credit, professional / academic, references and drug screenings. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 6.  | The organization will: (1) locate all production and disaster recovery data centers that store, process or transmit State of Minnesota data only in the continental United States, (2) store, process and transmit State of Minnesota data only in the continental United States, and (3) locate all monitoring and support of all the cloud computing or hosting services only in the continental U.S. | Yes [x] No [x] n/a [ ]  | Click here to enter text.     |
| 7.  | The system/solution/service provides password protection and security controls to prevent unauthorized access to or use of the system, data, and images. Proposed system solutions will ensure Industry best practices for security architecture & design. | Yes [x] No [x] n/a [ ]  | Click here to enter text.    |
| 8.  | The system/solution/service has capability to integrate with the State of Minnesota’s Identity and Access Management (IAM) system. | Yes [x] No [x] n/a [ ]  | Click here to enter text.     |
| 9.  | No data of any kind shall be transmitted, exchanged or otherwise passed to or accessed by other vendors or interested parties except on a case-by-case basis as specifically agreed to in writing by the State of Minnesota. | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 10.  | The system/solution/service will encrypt sensitive data in transit and at rest using industry standard encryption protocols; encryption keys will be managed at least in part by the State of Minnesota. | Yes [x] No [x] n/a [ ]  | Click here to enter text.     |
| 11.  | All data will be stored, processed, and maintained solely on designated servers and that no data at any time will be processed on or transferred to any portable or laptop computing device or any portable storage medium, unless that storage medium is in use as part of the organization’s designated backup and recovery processes. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 12.  | All Information systems will be configured to industry security best practices (e.g., CIS, NIST, etc.). | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 13.  | Anti-Malware software will be installed, running and maintained on all systems. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 14.  | All physical access to information systems will be controlled and restricted to only those with a need to physically access these systems. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 15.  | The system/solution/service will be developed according to secure software development best practices (e.g., OWASP, etc.). | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 16.  | Automated and manual software assurance assessment, testing and remediation processes are in place to detect security flaws in the underlying application code that could pose security risks.  | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 17.  | The system/solution/service has capability to integrate with the State of Minnesota’s Security Incident Event Management (SIEM) system. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 18.  | The system/solution/service’s storage processes, backup storage processes, and security procedures being implemented ensure that there is no loss of data or unauthorized access to the data. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 19.  | Firewalls are in place at the network perimeter and between the internal network segment and any DMZ. | Yes [x] No [x] n/a [ ]  | Click here to enter text.     |
| 20.  | Systems and applications are patched in a timely manner to ensure critical security and operational patches and fixes are in place to ensure the confidentiality, integrity and availability of the information system.  | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 21.  | Vulnerability tests (internal/external) are performed on all applications and platforms. | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 22.  | Online transactions must conform to reasonable commercial security standards and measures. Temporary files for all secure online transactions must be securely and permanently deleted when said transaction is complete | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 23.  | The system/solution/service will comply with the National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems and Organizations, Special Publication 800-53 revision 4, for Moderate systems. | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 24.  | Independent Security audits of the system/solution/service, processes and data centers used to provide the services/solution are conducted at least annually. Audits are performed in accordance to SSAE16 SOC 2 or equivalent (e.g. FedRAMP) industry security standards. Contracted vendor will provide the most recent independent physical and logical audit results to the State of Minnesota. | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 25.  | The organization will coordinate disaster recovery and business continuity processes and plans with the State of Minnesota and will provide the State of Minnesota with a detailed disaster recovery continuity of operations plan as part of their response. | Yes [x] No [x] n/a [ ]  | Click here to enter text.       |
| 26.  | The vendor must provide a detailed explanation of the security features that are built into the proposed system/solution/service. | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 27.  | The vendor and system/solution/product/ service/proposal will comply with the requirements of the Minnesota Government Data Practices Act/Minnesota Statutes chapter 13 and applicable federal laws/regulations (e.g., HIPAA, FERPA, IRS Publication 1075, FBI/CJIS)?  | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 28.  | If Federal, state or industry compliance requirements pertain to the data (e.g. CJI, IRS 1075, PHI (HIPAA), SSA, PCI, Etc.) the system/solution/service will comply with the said security policy and industry best practice. | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |
| 29.  | If CJI is in scope, organization staff (including employees, contractors and individuals working on behalf of the organization) that come in contact with CJI will pass an FBI fingerprinted background check and sign the FBI/CJIS Security Addendum/ Certification agreement | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 30.  | All data received from the State of Minnesota or created, collected or otherwise obtained as part of this agreement will be owned solely by the State of Minnesota and all access, use and disclosure of the data shall be restricted to only that which is required to perform the organization’s duties under this agreement. | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 31.  | Processes will be in place to securely destroy or delete State of Minnesota data according to the standards enumerated in D.O.D. 5015.2 from systems or media no longer being used to fulfill the terms of this agreement or upon request from the State of Minnesota.  | Yes [x] No [x] n/a [ ]  | Click here to enter text. |
| 32.  | In the event of termination of the agreement, the organization shall implement an orderly return of State of Minnesota assets and the subsequent secure disposal of State of Minnesota assets. During any period of suspension, the organization will not take any action to intentionally erase any State of Minnesota Data.  | Yes [x] No [x] n/a [ ]  | Click here to enter text.    |
| 33.  | An incident response plan is in place which includes notifying the State of Minnesota immediately of a known or suspected security or privacy incident involving State of Minnesota data. | Yes [x] No [x] n/a [ ]  | Click here to enter text.      |