Security Questionnaire

The purpose of this security questionnaire is to evaluate the security practices, features, and capabilities of vendors or service providers, specifically for the City of Virginia Beach. This questionnaire must be filled out by the vendor directly, not by City of Virginia Beach staff members. The questionnaire aims to gather detailed information about the vendor's security measures and determine if they meet the specific requirements and standards of the City of Virginia Beach. The main objectives of this security questionnaire are:

**Assessing Security Controls**: The questionnaire helps assess the effectiveness and adequacy of the security controls implemented by the vendor. It provides insights into the security features, authentication mechanisms, access controls, and data protection measures offered by the software.

**Identifying Compliance**: The questionnaire seeks to identify if the software complies with relevant security standards, regulations, and industry best practices. It helps determine if the vendor follows specific security frameworks or has obtained necessary certifications, ensuring that the software aligns with the City of Virginia Beach's compliance requirements.

**Evaluating Incident Response and Recovery**: The questionnaire assesses the vendor's incident response and disaster recovery capabilities. It aims to understand their processes for handling security incidents, notifying customers about vulnerabilities, and providing support during incident response and recovery.

**Vendor Due Diligence**: The questionnaire serves as a tool for conducting due diligence on potential vendors. It helps the City of Virginia Beach gain a deeper understanding of the vendor's security posture, vendor security policies, vendor infrastructure, and any third-party security audits or certifications they may have obtained.

Overall, the security questionnaire assists the City of Virginia Beach in making informed decisions regarding technology procurement, ensuring that the chosen vendor meets the security requirements, safeguards sensitive data, and mitigates potential security risks laid out in the City policies.

# Section 1: General

All the questions in section one must be answered in full, regardless of the solution type.

1. Please select which framework your information security program is based on: 
   1. If o*ther*, please list it here: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
2. What type of software solution are you providing? ****

*Based on your response here, please complete the corresponding section below. Only the applicable sections need to be filled out.*

1. What is your security patch and update cycle? ****
2. In the event of any data, network, or system breaches, can the vendor disclose to the City of Virginia Beach within 24 hours of the discovery of compromise the following information:
   1. *the nature of the event;*
   2. *length of compromise;*
   3. *suspected cause; and*
   4. *specific data and/or system that was accessed.*

Data breaches include the unauthorized access and/or loss of system, application, customer identifying, and/or financial data. ****

1. Does the software provide detailed documentation on security configuration and management? 
2. Are there specific system requirements or configurations needed to maintain security? ****

## Data Requirements

This section pertains to system, application, and identifying customer data (i.e., Names, Addresses, Financial information, etc.).

1. Will all data remain the sole ownership of the City of Virginia Beach? ****
2. Is all data kept in a format that allows for the City of Virginia Beach to request export of all City data held by the vendor at any time and for any reason? ****
3. If data is required to be destroyed, can the vendor perform physical destruction of private or restricted data? ****
   1. Will the City be able to obtain a certificate of data destruction as proof of compliance? ****
4. Do you share customer data with any third-party company for any reason? ****
   1. If yes, please detail whom the data partner is, what data is shared, the process for which the data is shared, all information security related agreements, and if compensation of any kind is provided in exchange for the data provided. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
5. Is the following information auditable: successful logins, unsuccessful login attempts, the IP address of the client system attempting access, and the date of the event and the time of the event with clearly identified time zone utilized. ****
6. Please attach all information security attestations and certification documentation held by the vendor for review by the City of Virginia Beach Information Technology department. Vendors must provide their own attestations. The use of cloud service provider attestations and certificates will not be accepted.
7. Please provide a point of contact for any follow up questions the City of Virginia Beach’s security team may have.

**Name**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Email**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**Phone Number**: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Section 2: SaaS/Cloud-based Solutions

SaaS (Software as a Service) and cloud-based solutions encompass a range of software applications and services that are delivered over the internet, rather than being installed on local computers or servers. This section includes all applications installed on desktops, laptops, servers, and mobile devices.

1. If the solution is classified as high-risk by an internal evaluation, do you consent to an initial external vulnerability assessment and an annual assessment every year thereafter? ****
2. All third-party vendors providing a technology solution not hosted within a City data center, City public cloud infrastructure or City private cloud shall maintain cyber security insurance in the following minimal amounts:
   1. $1 million USD per occurrence for vendors categorized as low risk.
   2. $3 million USD per occurrence for vendors categorized as medium risk; and
   3. $5 million USD per occurrence for vendors categorized as high risk.

Risk levels are determined by an internal audit. Please indicate your level of cyber security insurance: ****

## Encryption Requirements

1. Please select the option that corresponds with the highest current compatible encryption standard the application uses for all web and application transactions: ****
2. Please select the option that corresponds with the highest current compatible encryption standard the application uses for all database transactions:
   1. Data in-transit: ****
   2. Data-at-rest: ****
3. Do all supported encryption methods leverage the third-party vendor’s PKI or certificate management system? 
4. Does the technology require utilizing a certificate provided by the City of Virginia Beach as a product of its PKI or certificate management system? This includes a requirement to install any City of Virginia Beach certificate in a third-party vendors application security certificate store. ****

## Identity and Access

1. Does the technology leverage role-based access control (RBAC)? 
2. Does the technology leverage least privilege principles? 
3. Does the technology require service accounts or end user accounts to possess client or server system administrative rights? 
4. Does the technology leverage an identity management system such as Microsoft Active Directory or Open LDAP? ****

*If yes, please list the identity management system the technology is compatible with*:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Section 3: On-Premises/Locally Installed Solutions

On-Premises or Locally Installed Solutions refer to software applications and services that are installed and operated directly on the user's own hardware infrastructure, rather than being hosted and accessed via the internet. This section includes all applications installed on desktops, laptops, servers, and mobile devices.

1. Does the vendor provide support for incident response and recovery for on-premises solutions? ****
2. Does the software allow for the implementation of custom security policies and rules tailored to the City of Virginia Beach's requirements? ****
3. Does the software require specific hardware security modules (HSM) for key management? ****
4. Does the software support network segmentation to isolate sensitive data and systems? ****
5. Are there built-in defenses against common network attacks (e.g., DDoS, Man-in-the-Middle)? ****

*If yes, please identify the types of attacks and controls in place to eliminate or mitigate the risk of each attack type*:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Encryption Requirements

1. Please select the option that corresponds with the highest current compatible encryption standard the application uses for all web and application transactions: ****
2. Please select the option that corresponds with the highest current compatible encryption standard the application uses for all database transactions:
   1. Data in-transit: ****
   2. Data-at-rest: ****
3. Do all supported encryption methods leverage the third-party vendor’s PKI or certificate management system? ****
4. Does the technology require utilizing a certificate provided by the City of Virginia Beach as a product of its PKI or certificate management system? This includes a requirement to install any City of Virginia Beach certificate in a third-party vendors application security certificate store. ****

## Identity and Access

1. Does the technology leverage role-based access control (RBAC)? ****
2. Does the technology leverage least privilege principles? ****
3. Does the technology require service accounts or end user accounts to possess client or server system administrative rights? ****
4. Does the technology leverage an identity management system such as Microsoft Active Directory or Open LDAP? ****

*If yes, please list the identity management system the technology is compatible with:*

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Section 4: Open-Source Programs, Plugins, Drivers, & Programming Languages

1. Is there a dedicated security team responsible for addressing vulnerabilities? ****
2. Please list the team’s contact info if available
   * 1. ***Team Name***: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     2. ***Point of Contact***: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     3. ***Email***: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
     4. ***Phone Number***: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_
3. Please describe your vulnerability disclosure process below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. How regularly is the source code audited for security vulnerabilities? ****
2. How do you handle updates and security issues for any third-party libraries?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Please describe your third-party library vulnerability disclosure process below:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. What guidelines or best practices are utilized to ensure secure coding? (**Check all that apply**)

|  |  |
| --- | --- |
| OWASP Secure Coding Practices | NIST Secure Software Development Framework (SSDF) |
| SANS Secure Coding Guidelines | CERT Secure Coding Standards |
| ISO/IEC 27034 Application Security Guidelines | CIS (Center for Internet Security) Benchmarks |
| PCI DSS Secure Software Requirements | Microsoft Secure Development Lifecycle (SDL) |
| Google's Application Security Best Practices | GitHub's Secure Coding Practices |
| Use of secure coding libraries and frameworks | Automated static analysis tools |
| Regular code reviews and security assessments | Threat modeling and risk assessments |
| Dynamic analysis tools | Regular security updates and patch management |
| Continuous integration/continuous deployment (CI/CD) security practices | Other |

If other is selected, please describe:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

## Programming Languages/Libraries

These questions are specific to programming languages and/or libraries.

1. Which built-in security features are present? (**Check all that apply**)

|  |  |
| --- | --- |
| Input validation | Output encoding |
| Secure memory management | Encryption libraries |
| Secure random number generation | Access control mechanisms |
| Role-based access control (RBAC) | Multi-factor authentication (MFA) |
| Auditing and logging capabilities | Protection against SQL injection |
| Protection against cross-site scripting (XSS) | Protection against cross-site request forgery (CSRF) |
| Secure session management | Secure API development practices |
| Data masking | Data integrity checks |
| Built-in compliance with security standards (e.g., OWASP, NIST) | Automated security testing tools |
| Code signing | Secure boot |
| Container security | Network security controls |
| Sandbox environments for testing | Secure file handling |
| Other |  |

If other is selected, please describe:

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

1. Please describe process for reporting and fixing security issues if they are discovered by users or the community, including links and or contact information. \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_