|  |
| --- |
| **Software as a Service (SaaS) Provider**  **Information Security and Privacy Assessment Questionnaire** |
| Purpose: This form is to be used to conduct security assessment on Vendor  Note/Instructions:   * The Software as a Service (SaaS) is a software distribution model in which applications are hosted by a vendor or service provider and made available to customers over a network, typically the Internet. * This document is for the sole use of the intended recipient(s) and may contain confidential and privileged information belongs to SAWS. Any unauthorized review, use, disclosure or distribution is prohibited. If you are not the intended recipient, please contact the sender by reply email and destroy all copies of the original message. * The Vendor shall provide answers or information to the questions or statements below. * In the event that the Vendor cannot meet SAWS security and or privacy requirements, the Vendor may submit an exception with alternative countermeasures to address the risk. SAWS Network Security Services Manager may approve or reject the exception request depending upon the risk associated with the exception request. * Followed by the Vendor’s response SAWS Network Security Services will conduct a security risk assessment with following scoring methodology:   **A = Meet completely,**  **B = Partially meets. The Vendor may require to provide additional requested details**  **C = Doesn’t meet. The Vendor may require to provide missing/additional detail.** |

**The Vendor’s Information:**

|  |  |
| --- | --- |
| Vendor’s Organization Name |  |
| Address |  |
| Information Security Contact Person Name |  |
| Email |  |
| Phone |  |
| Date this Questionnaire Completed |  |

**1.0 BUSINESS PROCESS AND DATA EXCHANGE REQUIREMENTS**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 1.1 | Please provide a detailed description of the business process that will be supported by the Vendor as it relates to the requirements of the RFP |  |  |  |
| 1.2 | Has Vendor adopted and implemented information security and privacy policies that are documented, are accessible to SAWS and conform to ISO 27001/2 – Information Security Management Systems (ISMS) Standards or other industry standards. |  |  |  |
| 1.3 | What data exchange needs to occur between SAWS and the Vendor? What data will be stored at the Vendor location? (Provide data attributes with examples)  Example: (PCI Credit Card Info, SSN, DLN, Patrons Name, Address, telephone, employee performance data, etc.) |  |  |  |
| 1.4 | In the event that Vendor is required to store Private Information (PI) or Personally Identifiable Information (PII) or Sensitive Information (SI) about peoples in the Vendor’s business systems -- how will the Vendor maintain the confidentiality of the Information in accordance with applicable federal, state and local data and information privacy laws, rules and regulations. |  |  |  |
| 1.5 | What mechanism and/or what types of tool will be used to exchange data between SAWS and the Vendor? Example: (VPN, Data Link, Frame Relay, HTTP, HTTPS, FTP, FTPS, etc.)? What versions of SSL are used? |  |  |  |
| 1.6 | What types of data Storage (work in progress storage and backup storage) will be required at the Vendor site Example: (PCI Credit Card Info, SSN, DLN, Patrons Name, Address, telephone, employee ID number, HR evaluation data, etc.) |  |  |  |
| 1.7 | Is there any e-mail integration required between SAWS and the Vendor?  Example: The vendor may require an e-mail account on SAWS e–mail Server. |  |  |  |
| 1.8 | Will any integration with ERP systems be required and how will the data be exchanged, e.g. HR, Finance, etc.? |  |  |  |
| 1.9 | Has the Vendor ever been subjected to either an electronic or physical security breach? Please describe the event(s) and the steps taken to mitigate the root causes. What damages or exposure resulted? Are records of breaches and issues maintained and will these records be available for inspection by SAWS? |  |  |  |
| 1.10 | Does the Vendor maintain formal security policies and procedures to comply with applicable statutory or industry practice requirements/standards? Are records maintained to demonstrate compliance or certification? Does the Vendor allow client audit of these records? NOTE: PLEASE PROVIDE SUPPORTING DOCUMENTATION. |  |  |  |
| 1.11 | What are the internet and the browser security configuration of the vendor application? What security standards and requirements are maintained to ensure application security at the user interface? (A set of detailed documentation should be provided to support the compliance. |  |  |  |

**2.0 APPLICATION/SOLUTION CONFIGURATION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 2.1 | What is the name of the application the Vendor will host to provide services to SAWS? (List all) Is the application on-premise or hosted? |  |  |  |
| 2.2. | What functionality will be provided to SAWS employees or SAWS customers through the application? |  |  |  |
| 2.3 | Is the Vendor using a subcontractor or 3rd party service provider? (List all). If yes, then what data privacy and information security agreements are in place between the Vendor and any subcontractor to ensure appropriate and accountable treatment of information. Also SAWS requires that this questionnaire shall be completed by each subcontractor as well. |  |  |  |
| 2.4 | What is the Vendor's Application hosting hardware and software platform? Also please provide detailed description including SP and a patch or security applications in use  Example: Windows or Unix Operating System (OS) and other detail |  |  |  |
| 2.5 | How do the Vendor’s application and database architecture; manage segregation of SAWS data, from other customers' data? |  |  |  |
| 2.6 | Describe the Vendor’s server and network infrastructure. Please provide server and network infrastructure deployment topology, including data flow architecture including but not limited to security management applications, firewalls, etc. |  |  |  |
| 2.7 | Please provide detail proposed solution which will be developed as a part of the implementation to support this project. (For example detailed solution architecture, secured data flow to support business processes, etc.). |  |  |  |

**3.0 DATA PROTECTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 3.1 | How is SAWS data kept physically and logically secure at the Vendor location? Example: Locked storage, Digitally, Encrypted etc. If encrypted please provide the encryption standard used. How are keys kept separated from the data? |  |  |  |
| 3.2 | What application level protections are in place to prevent vendor/Vendor or subcontractor staff from being able to view protected information i.e.: encryption, masking, etc.? |  |  |  |
| 3.3 | What controls does the Vendor exercise over the qualification and performance of their team? Of their subcontractor’s teams? (For example criminal background verification prior to employment, providing security training after employment and managing Role Based Access Control (RBAC) during employment and network and application access termination upon employment termination. |  |  |  |

**4.0 DATA BACK-UP**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response** | **Score** | **SAWS’s Security Assessment** |
| 4.1 | What method is used to keep data secure during backup process? |  |  |  |
| 4.2. | Is encryption technology used to encrypt; whole, or selective data? If so, how is the data encrypted? |  |  |  |
| 4.3 | What types the “media” used for data backup (Tape, Hard Disk Drive or any other devices)? |  |  |  |
| 4.4 | Are the backups encrypted? If yes, please provide encryption specification, with type of encryption algorithm and detail process of encryption handling. If No, please provide detail description (with process, tools and technology) to keep data secured during the back-up process. |  |  |  |

**5.0 DATA RETENTION**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 5.1 | What is the retention period for the data being backed up? The data retention process shall comply with SAWS data retention policy. |  |  |  |
| 5.2 | Are the data back-up tapes/media stored at the Vendor location or off-site? |  |  |  |
| 5.3 | If the Vendor’s backups are stored with another company, please provide:   1. Company Name: 2. Address: 3. Contact person detail (Phone and Email): 4. What contractual commitments are in place to guarantee security performance from these vendors |  |  |  |
| 5.5 | What is the media transfer process (I.e. The lock box process used to send tapes off-site)? |  |  |  |
| 5.6 | Who has access to the media lockbox? (Provide Name and Role) |  |  |  |
| 5.7 | Who is authorized to access back-up media? (Provide Name and Role) |  |  |  |
| 5.8 | What is the backup media receiving and release authorization process? (Please submit a soft copy of the process) |  |  |  |

**6.0 ACCOUNT PROVISIONING AND DE-PROVISIONING (The Vendor must receive formal pre-authorization from the City’s Information Security Manager prior to provisioning and de-provisioning of application access account).**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 6.1 | What is the account provisioning/removal process?  Example: how are users accounts created and managed?) |  |  |  |
| 6.2 | What is the account deprovisioning/removal process? Example: how are users accounts created and managed?) |  |  |  |
| 6.3 | How will SAWS employees gain access to required application(s)? |  |  |  |
| 6.4 | Does the application(s) have the capability to restrict access only from SAWS network? |  |  |  |

**7.0 PASSWORD MANAGEMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 7.1 | What will be the Policy and Procedures for the logging, authentication, authorization and password management scheme? (Pleaseprovide a soft copy of the process) |  |  |  |
| 7.2 | Where are the login and password credentials stored? |  |  |  |
| 7.3 | Are the password credentials stored with encryption? If yes please provide encryption scheme detail. |  |  |  |
| 7.4 | The vendor application must comply with following password requirements. Does the vendor application meet these requirements:   1. First time password must be unique to an individual and force the user to change it upon initial login. 2. How is a forgotten or expired password changed by the customer? 3. SAWS requires first time password to have a time-out capability of no more than 7 days. 4. The email notification must not be CC’d to anyone else except the user. 5. The permanent / long term password must be changed frequently, at least TWICE a year 6. E-mail notification must be sent to the user whenever the password has been updated. 7. User should not be able to view data or conduct business unless an initial password has been updated with a different password. 8. The Vendor shall notify SAWS users; that when creating a new password, the user shall not use their SAWS LDAP password. 9. Account must be able to be locked out after a defined number of failed logon attempts. To be defined by SAWS. 10. The password must have 8 characters or more and they must contain at least one character from each line below i.e. each line shall contribute at least one character:  * abcdefghijklmnopqrstuvwxyz * ABCDEFGHIJKLMNOPQRSTUVWXYZ * 0123456789 * !@#$%^&\*()-+=`~,></\"'?;:{[}] |  |  |  |
| 7.5 | Does the Vendor support or provide Single Sign On capabilities? If so please explain how. Does the vendor support SAML 2.0? |  |  |  |
| 7.6 | Does the Saas vendor support two factor authentication and if so how? |  |  |  |

**8.0 AUDIT MANAGEMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 8.1 | Is access to SAWS data audited? |  |  |  |
| 8.2 | What events are audited, access, modification, etc., and to what level? |  |  |  |
| 8.3 | What is the retention policy for audit logs? |  |  |  |
| 8.4 | Will SAWS be able to get access to audit logs and what is the procedure and timeline? |  |  |  |

**9.0 CONFIGURATION MANAGEMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 9.1 | What is the vendors configuration/change control policy? |  |  |  |
| 9.2 | How are customers notified of system updates? |  |  |  |
| 9.3 | What is the process for applying critical updates, e.g. Heartbleed? |  |  |  |
| 9.4 | Is the vendor application vulnerability tested by a third party? |  |  |  |

**10.0 INCIDENT MANAGEMENT**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **#** | **Question** | **Response from Vendor** | **Score** | **Additional Information/Clarification Required from Vendor** |
| 10.1 | Does the vendor have an incident response policy and can SAWS get a copy? |  |  |  |
| 10.2 | What is the vendor’s timeline to notify customer of a potential breach? |  |  |  |

--------------------------------------------------- End Of Document --------------------------------------------------