City of Phoenix

INFORMATION SECURITY
RISK ASSESSMENT QUESTIONNAIRE

(Third-Party Assessment, BIRF Submissions, RFP/RFI Evaluations)

V1.3.

NOTE: *Completed copies of this questionnaire should be sent to the Information Security & Privacy Office at ispo@phoenix.gov. Department Staff/Project Managers who are responsible for RFP/RFI and/or BIRF submissions should work with their Department Procurement Officers for assistance in completing this form. This form may be provided to Vendor contacts to answer as many questions as possible. Questions are based on information security best practices. Contact ISPO if additional help is required.*

Vendor Name:_____ **Assessment Date:** _____

Address:_____ **Website**: _____

Vendor Contact: _____**Email**:_____ **Phone:** _____

Department: _____**Contact:**_____ **Phone:**_____

Description of Service/Product:_____

Intended Users of the Service/Product *(City staff, Contract Staff, Volunteers, Business Partners, Etc.)*_____

Describe Contracted Servicing Arrangements *(onsite support, remote support, temporary access , database management, etc.):*

DATA REQUIREMENTS

(mark a "1" in all boxes applicable for this relationship)

Data Stored on City Servers	Data Stored in Cloud	*Risk*	*Data Type (if needed, refer to definitions worksheet tab)*	ISPO Comments
		High	Protected Health Information (PHI)	
		High	Personally Identifiable Information (PII)	
		High	Social Security Numbers (SSN)	
		High	Payment Card Information (PCI)	
		High	Criminal Justice Information (CJI)	
		High	Restricted City Information (RCI)	
		Medium	City of Phoenix Staff Working Papers	
		Low	Public Information	

Answer: 0 = Not Applicable, based on service provided
1 = Yes
2 = Partially
3 = No

Comments: Optional, but may be used to explain answers.

Answer	Comments	**A. Cloud Data Security.** **The vendor(s):**	ISPO Comments
		1. Will accommodate an onsite visit for a security audit.	
		2. Will store City confidential data (CJI, PCI, PHI, PIII, RCI, etc) within Continental US - including backups.	
		3. Application/service is hosted on a certified government cloud (Microsoft Azure, Amazon AWS GovCloud, etc.)	

		4. Is aware of City requirements for documented cloud exit strategies including recovery/destruction of data and verification by contractor; data ownership, and allotted timeframes for City of Phoenix data to be returned to the City in an approved data format. (These proposals must be vetted by the LAW Department prior to contract signing.)	
		5. Agrees to follow City Data Security and Confidentiality contract clause.	
		6. Will provide City with results of a third-party external Information Security assessment (SAS-70, SSAE-16/18, penetration test, vulnerability assessment, etc.) other Statement of Controls (SOC) reports.	
0		***Total Company Controls***	
Answer	**Comments**	**B. Polices, Standards and Procedures. The vendor(s):**	**ISPO Comments**
		1. Has formal written Information Security Policies.	
		2. Can provide results of a third-party external Information Security assessment (SAS-70, SSAE-16/18, penetration test, vulnerability assessment, etc.).	
		3. Has a policy to protect client information against unauthorized access; whether stored, printed, spoken or transmitted.	
		4. Has a policy that prohibits sharing of individual accounts and passwords.	
		5. Performs background checks for individuals handling confidential information.	
		6. Has termination or job transfer procedures that immediately protect unauthorized access to information.	
		7. Has documented change control processes.	
		8. Requires contractors, subcontractors, vendors, outsourcing ventures, or other external third-party contracts to comply with policies and customer agreements.	
		9. Implements Information Security awareness training for vendor staff, sub-contractors.	
0		***Total Policy Controls***	
Answer	**Comments**	**C. Architecture. The vendor(s):**	**ISPO Comments**
		1. Will provide a network topology diagram/design.	
		2. Implements network firewall protection, web application firewall protection and host intrusion fire wall protection.	
		3. Has IDS/IPS technology implemented.	
		4. Uses DMZ architecture for Internet systems.	
		5. Uses enterprise virus protection on all systems.	
		6. Follows a program of enterprise patch management.	
		7. Ensures that remote access is only possible over secure connections.	
		8. Uses separate physical and logical development, test and production environments and databases.	
0		***Total Architecture Controls***	
Answer	**Comments**	**D. Configurations. The vendor(s):**	**ISPO Comments**
		1. Implements encryption for confidential information being transmitted on external or Internet connections with a strength of at least AES 256 bit and uses TLS 1.2. (mandatory for web applications). IPSEC is an option for those providers that support site to site VPN in addition to TLS 1.2.	
		2. Implements encryption for confidential information at rest with a strength of at least AES 256 bit.	
		3. For encrypted solutions implements key management including off site storage, key escrow, etc.	
		4. Uses file integrity monitoring software on servers.	
		5. Changes or disables all vendor-supplied default passwords or similar “published” access codes for all installed operating systems, database management systems, network devices, application packages, and any other commercially produced IT products.	
		6. Uses passwords that are a minimum of 8 characters, expire at least annually.	
		7. Sets the account lockout feature for successive failed logon attempts on all system's support computers.	
		8. Prohibits split tunneling when connecting to customer networks.	
0		***Total Configuration Controls***	
Answer	**Comments**	**E. Product Design. The vendor(s):**	**ISPO Comments**

		1. Ensures that if the product integrates with portable devices, confidential information is encrypted when stored on these portable devices and requires password access.	
		2. Implements protections for CVEs in a timely manner to protect from exploits.	
		3. Audits the application against the OWASP Top 10 Application Security Risks.	
		4. Ensures that application server and database software technologies are kept up-to-date with the latest security patches.	
		5. Performs security code reviews as part of their SDL.	
0		***Total Product Design Controls***	
Answer	**Comments**	**F. Compliance. The vendor(s):**	**ISPO Comments**
		1. Can provide documentation of HIPAA compliance if system/service stores PHI data.	
		2. Can provide documentation of PCI-DSS compliance if vendor system/services stores, transmits or processes PCI cardholder data.	
		3. Uses industry standard best practices for application security (e.g. OWASP).	
0		***Total Product Design Controls***	
Answer	**Comments**	**G. Access Control. The vendor(s):**	**ISPO Comments**
		1. Immediately removes, or modifies access, when personnel terminate, transfer, or change job functions.	
		2. Assigns unique IDs and prohibiting password sharing.	
		3. Implements least privilege access only giving a user account those privileges which are essential to perform its intended function	
0		***Total Access Controls***	
Answer	**Comments**	**H. Monitoring. The vendor(s):**	**ISPO Comments**
		1. Reviews access permissions for all server files, databases, application, etc.	
		2. Implements system event logging on all servers and records at a minimum who, what, and when for all transactions.	
		3. Reviews system logs for failed logins, or failed access attempts.	
		4. Reviews web server logs for possible intrusion attempts.	
		5. Reviews network and firewall logs.	
		6. Performs scanning for rogue wireless access points.	
		7. Performs vulnerability scanning.	
		8. Performs penetration testing.	
0		***Total Monitoring Controls***	
Answer	**Comments**	**I. Physical Security. The vendor(s):**	**ISPO Comments**
		1. Controls access to secure areas.	
		2. Has special safeguards in place for computer rooms (e.g. cipher locks, restricted access, room access log, card swipe access control, etc.)	
		3. Prohibits or encrypts confidential information on laptops & mobile devices.	
		4. Escorts all visitors in computer rooms or server areas.	
0		***Total Physical Controls***	
Answer	**Comments**	**J. Contingency. The vendor(s):**	**ISPO Comments**
		1. Has written backup procedures and processes.	
		2. Maintains a documented and tested disaster recovery plan.	
		3. Uses off-site storage and has documented retrieval procedures for backups.	
		4. Password protects and encrypts all backups.	
0		***Total Contingency Controls***	