

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

General Questions	Answer	Follow-Up Question	Answer
Please provide a brief overview of your product/solution?			
Are there any technical documents available to review? (Yes/No)		Please provide those documents.	
How long has this solution been available on the market?			
How many customers are actively using this solution?			
What is your development roadmap for the next 12-24 months?			
Outline the typical process and timeline for implementing your product/solution with a new customer.			
Do you offer "turnkey" installation/configuration? (Yes/No)			
What is the customer's level of involvement for a full implementation/configuration?			
How do you handle software updates, how often are they released, and how do you notify customers?			
Who controls pushing new updates? (Customer or Vendor)			
What additional hardware is required (printers, card readers, tablet holders, etc.)?			
Can the application work offline? (Yes/No)		Please explain any additional requirements, stipulations, or limitations (e.g. licenses, hosted server, limited functions etc.)?	
How do you handle data migration from an existing solution?			
Are there custom reporting capabilities? (Yes/No)		If yes, please explain the reporting capabilities.	
Can the end user import data? (Yes/No)			
Can the end user export data? (Yes/No)			
Does your product/solution use any payment processors? (Yes/No)		If yes, which payment processors are used with in your product/solution?	

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

What types of data will your product or solution store or process on behalf of our organization? (Select all that apply) Criminal Justice Information Services (CJIS) Data, Critical Infrastructure Information, Financial Information, Geospatial, Intellectual Property, Management and Support Information, Mission-Based Information, Operational Information Personally Identifiable Information (PII), Protected Health Information (PHI), Security Management Information, Other: Please explain		If other, please explain.	
Is your product, whether website or mobile application, public facing? (Yes/No)		If yes, Is your product, whether website or mobile application, fully compliant with WCAG 2.1 Level AA accessibility standards? (Yes/No)	
		If yes, Please upload Voluntary Product Accessibility Template (VPAT) or Accessibility Conformance Report (ACR) (attach document)	
		If No, Why is your product not compliant with WCAG 2.1 Level AA accessibility standards?	
Is there any Supplemental information that you can provide?			
Support Questions	Answer	Follow-Up Question	Answer
Where are your support centers located?			
What are your support hours?			
Do you offer after hours support? (Yes/No)			
What is the process by which high, medium, and low priority technical issues can be reported? What classifies each priority level?			
What is your process and response time for handling each priority of technical issues (high, medium, and low)?			
Describe the escalation process for critical issues and expected response times.			
What are the method(s) of notification for outages and planned maintenance?			
Training Questions	Answer	Follow-Up Question	Answer

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

What kind of training is available for the product/solution (e.g., webinars, videos, guides, “train the trainer”)?			
--	--	--	--

Purchasing Questions	Answer	Follow-Up Question	Answer
Provide details regarding your pricing model.			
What are the standard contract terms and service level agreements (SLAs) that clients can expect?			
Is this a proprietary/sole-source solution? (Yes/No)		If yes, please provide documentation.	
Is your product available on any Federal, Cooperative, or Florida State contract (e.g. NASPO, Source Well, GSA)? (Yes/No)		If yes, please explain.	
How long has your company been in business, and what is your financial stability?			
Are there any recent or planned major changes within the company that could affect your ability to support clients (e.g., acquisitions, mergers, or pending litigation)?			
Please provide any supplemental or supporting documentation from the questions you answered on this questionnaire.			
Describe your licensing model (e.g., concurrent, per user, per site).			
Do you have a standard annual rate increase? (Yes/No)		If yes, is this increase typically locked in for the life of the contract?	

General Security - Vendor Environment Questions	Answer	Follow-Up Question	Answer
Does your organization perform background checks on employees with access to sensitive data? (Yes/No)		If no, please explain why.	
Does your organization provide security awareness training to all employees and contractors? (Yes/No)		If no, please explain why.	
Does your organization implement least privilege access controls? (Yes/No)		If no, please explain why.	
Does your organization enforce multi-factor authentication (MFA) for all user accounts, especially privileged accounts for managing client data? (Yes/No)		If no, please explain why.	
Does your organization maintain a comprehensive asset inventory, including hardware, software, and data? (Yes/No)		If no, please explain why.	

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

Does your organization have a process for securely disposing of data and hardware? (Yes/No)		If no, please explain why.	
Does your organization encrypt client data at rest and in transit? (Yes/No)		If no, please explain why.	
Does your organization have a process for secure configuration management of systems and applications? (Yes/No)		If no, please explain why.	
Does your organization monitor network traffic for suspicious activity? (Yes/No)		If no, please explain why.	
Does your organization have a process for logging and auditing security-related events? (Yes/No)		If no, please explain why.	
Does your organization have a data backup and recovery plan that is regularly tested? (Yes/No)		If no, please explain why.	
Does your organization have a documented process for managing third-party access to your systems and data? (Yes/No)		If no, please explain why.	
Does your organization comply with relevant industry standards and regulations (e.g., ISO 27001, SOC 2, PCI DSS, HIPAA, NERC, EPA)? (Yes/No)		If no, please explain why.	
Does your organization have a process for regularly reviewing and updating its security controls based on changes in the threat landscape? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking software vulnerabilities and its related security patch? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking hardware vulnerabilities? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking security exceptions? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking configuration changes? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking security alerts and events? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking security vulnerabilities in its applications? (Yes/No)		If no, please explain why.	

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

Does your organization have a process for ensuring the integrity of its software and data? (Yes/No)		If no, please explain why.	
Does your product or solution utilize any hardware, software or communications equipment that are included on the FCC's Covered List, as defined by Section 1.50002 of the Commission's rules under the Secure and Trusted Communications Networks Act of 2019? (Yes/No)		If yes, please explain why.	
Is this a hosted or on-premises product/solution? (Hosted, On-Premise, Could be either)		If Hosted or Could be either, please proceed to the Cloud Security Questions. If on-premise, please proceed to Incident Response Questions.	

Cloud Security Question	Answer	Follow-Up Question	Answer
Does your organization have a process for ensuring the security of its APIs? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and tracking security vulnerabilities in its cloud infrastructure? (Yes/No)		If no, please explain why.	
Does your organization have a business continuity plan that addresses potential disruptions to its cloud services? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud storage? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud compute resources? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud network? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud identity and access management? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud monitoring and logging? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud key management? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud data loss prevention? (Yes/No)		If no, please explain why.	

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

Does your organization have a process for ensuring the security of its cloud intrusion detection and prevention? (Yes/No)		If no, please explain why.	
Does your organization have a process for ensuring the security of its cloud security information and event management (SIEM)? (Yes/No)		If no, please explain why.	
Does your product/solution have a test environment? (Yes/No)		If no, please explain why.	
For hosted solutions, can customers restrict the solution and data to reside only in data centers located within the United States, or does this hosted solution run on US government cloud resources? (Yes/No)		If no, please explain why.	

Incident Response Question	Answer	Follow-Up Question	Answer
Does your organization have a documented Information Security Policy that is reviewed and updated annually? (Yes/No)		If no, please explain why.	
Does your organization have a process for communicating security incidents to affected parties? (Yes/No)		If no, please explain why.	
Does your organization have a process for conducting forensic investigations of security incidents? (Yes/No)		If no, please explain why.	
Does your organization conduct regular risk assessments to identify and prioritize security risks? (Yes/No)		If yes, what is the frequency? If no, please explain why.	
Does your organization perform regular vulnerability scanning and penetration testing? (Yes/No)		If yes, what is the frequency? If no, please explain why.	
Does your organization have a formal incident response plan that is tested annually? (Yes/No)		If no, please explain why.	
Does your organization have a process for managing and responding to data breaches? (Yes/No)		If no, please explain why.	
Has your company experienced any data breaches? (Yes/No)		If yes, describe when it occurred, what the circumstances were, and corrective action(s) taken.	

Application Security questions			
Does the application support multiple security roles with granularity (e.g., clear separation of admin and standard user roles)? (Yes/No)			

Exhibit A - City of Ocala - IT Vendor Assessment Questionnaire Sample

Does your product/solution integrate with Microsoft Active Directory for Single Sign On (SSO) (e.g., SAML, ADFS)? (Yes/No)			
Does your product/solution support the use of multi-factor authentication (MFA) for client accounts? (Yes/No)			
Does your product/solution use any third-party software, libraries, or open source components? (Yes/No)		What is the software?	

References: Please provide at least three (3) customer references, preferably Florida municipalities or in Florida.			
Please provide the contact information for the individual completing this questionnaire.			
Please provide any additional information or details that you believe are valuable for us to know.			
Reference 1 {Please include a Company name, Contact Person, Phone Number, Email, and Length of Business Relationship}			
Reference 2 {Please include a Company name, Contact Person, Phone Number, Email, and Length of Business Relationship}			
Reference 3 {Please include a Company name, Contact Person, Phone Number, Email, and Length of Business Relationship}			