City of Asheville Technology Procurement Governance Checklist

Last revised 7/1/2024

NOTE: This tab is publicly accessible here. Please feel free to share with potential vendors.

	Item	Questions	Why is it important?	Vendor Response
☐	Data Ownership	Does the City retain ownership of all data in the system? Does the vendor have rights to use the data that users would be uncomfortable with?	We need to retain ownership so that we can transfer data and continue to satisfy public records requests after we change vendors.	
☐	Data Privacy	Does the vendor have an expectation of using any customer data? If so, what data and how? Does the system maintain data that users would consider private or sensitive, such as social security or credit card numbers, address, location of use, etc.?	Vendor use of employee or community members' data can easily erode trust in the City. Data that, if breached, subjects users to identity theft, harrassment, or exploitation may be subject to special regulation and always requires higher levels of security and governance.	
☐	Data Standards	Is there an applicable data standard that should be used (e.g. GTFS, Open311)?	Open standards facilitate interoperability with other systems and can also help ease the transition when changing vendors.	
☐	Open, Published APIs	Are push and pull APIs available for integrations and reporting?	Open APIs provide the foundation for automation, integration and reporting. They are no longer a nice-to-have feature, but an expected part of any modern application.	
☐	Financial integration	If the system involves any fees or charges, what methods does the vendor offer for integration into the City's financial system?	Automation increases the speed and accuracy of posted financial transactions into the general ledger and eliminates manual entry of transactions.	
☐	Other Data Integration Needs	Does the system need to integrate with GIS, workorder, or other enterprise systems?	Most applications support part of a workflow that may involve other enterprise systems besides financial ones. It is important that we be able to automate the interactions between different parts of the workflow.	
☐	Accessibility	Does it comply with the Web Content Accesbility Guidelines? If so, which version of the WCAG standard? Describe any testing that has been done to ensure compliance with the WCAG standard. Please provide a copy of your Voluntary Product Accessibility Tempate (VPAT).	As government, we must serve all of our community. We acknowledge that a large percentage of users experience temporary or permanent disabilities. The 2024 ruling on accessibility by the Department of Justice (https://www.ada.gov/resources/2024-03-08-web-rule/) defines the technical standard for any web and mobile apps provided by local and state governments. These generally must comply with the WCAG 2.1, Level AA standard.	
☐	Software Usability & Responsive Design	How do you measure usability of your product/service? Is your product designed to work on any size device (phone, tablet, workstation)?	Users draw conclusions about an organization based on every interaction, including digital ones. With the public, bad interfaces tend to undermine trust in the organization. With current and future employees, our digital interfaces are a key part of our "curb appeal" and can impact how readily we can recruit and retain talent.	
☐	Equity and Digital Inclusion	What steps have been taken to ensure that the proposed / services do not create inequitable impacts?	Technology projects can create inequitable access or outcomes particularly if no questions are asked (e.g. facial recognition technologies are not always designed for different skin tones).	
☐	Exit strategy (avoid lock-in)	What is the process for getting data and transferring to a new vendor? In what format will data be made available, how often can the City access, and is there a cost?	All systems have a useful lifetime after which we must be able to move to a new solution and the cost of that move is a critical component of the total cost of ownership of the system. Further, in the event of poor performance, an inability to get and move the data dramatically reduces our leverage in holding vendors accountable.	
☐	Data Center Security (SaaS)	What security standards does the vendor implement to ensure data cannot be breached? Does the company have a dedicated security team? Has the vendor ever had a breach? What framework are the vendor services built on? Is the vendor CJIS compliant or worked with CJIS integrated data before?	Knowing what security framework the data center is built on lets us know and follow the standards they have in place. This also helps with possible CJIS, HIPAA, and PII data integration or systems that access this data and the sensitivity of this data.	

City of Asheville Technology Procurement Governance Checklist

Last revised 7/1/2024

NOTE: This tab is publicly accessible here. Please feel free to share with potential vendors.

	Item	Questions	Why is it important?	Vendor Response
☐	PCI Compliance	Are credit card payments going to be processed through the software/website/app?	Credit card information is subject to specific legal requirements. Review with Finance to ensure compatibility with existing City of Asheville finance systems.	
☐	Single Sign On (SSO) Options	Describe options provided for single sign on. e.g. Google authentication and Azure AD.	To improve overall security, single sign on options are preferred to avoid a proliferation of inconsistent usernames and passwords. SSO also facilitates license managment when user accounts need to be suspended.	
☐	Data backup and disaster recovery	What is the vendor strategy to ensure that no data is lost in the case of system failure? What is the strategy for continuation of operations in the case of a disaster?	Disasters and system failures can and will occur and it is critical that all our systems implement backup and recovery strategies that allow us to continue vital operations and to recover normal operations as quickly and as easily as possible.	
☐	Service Level Agreement	Does an SLA exist and is it adequate for our business needs? Please provide a copy of your SLA with your response.	It is important that we and the vendor have clear, shared expectations of how quickly the vendor will respond if problems occur. Not every system requires rapid response, but some do and it's important to ensure that the promised service level aligns with our business requirements.	
☐	On-Premise infrastructure requirements	Are there any needs for on-premise storage, servers, etc?	The City of Asheville is working to minimize its data center footprint and migrate to hosted services.	
☐	Access needed to on-premise infrastructure or to our network	Does the vendor or do vendor systems require access to our internal network? How does the vendor make a connection to our data center? Are these connections from one location or multiple locations?	Allowing outside vendor connections into our network increases the risk of a 3rd party breach and infection of our systems.	
☐	Administrative Rights	Does this product allow the IT Services Department to have Administrative Rights to the software?	In some situations, IT Services needs to have administrative access to the software In order to fully support the end user and to be able to work with vendor support.	
☐	Data Encryption	Is data encrypted both while in transit and when at rest (client side and/or server side)? Can vendor's employees view the stored data or files?	Prevents sensitive data from being intercepted while in transit. Without internal access controls a vendor's employees can view or copy unencrypted agency data that is stored	
☐	Licensing Model	Describe your software licensing model. Is it subscription-based (frequency)? If not subscription based, are the licenses honor-based, concurrent, floating or fixed, etc. Is a license server required. Named user versus global license	Does the server need to check online when starting to validate its license. Is a license server required? Is authentication hardware (i.e. dongle) needed?	