**Software Acquisition Requirements**

# I. SOFTWARE AND SYSTEMS

**a. General**

1. ADA Compliance. ADA Law Accessibility & Compliance – Indicate how software is or will meet the Priority 1 checkpoints of the Web Content Accessibility Guidelines 1.0 (<https://www.w3.org/WAI/>) outlined by the W3C. In the event that a particular page or feature of your application is not WCAG Level 1.0 compliant, explain how you will provide an alternative, compliant page. Indicate if current application compliant with U.S. Section 508 (29 U.S.C. ‘794d) (See <https://www.section508.gov/test>). Provide a version of each Code you host for Disability Access, accessible via your mobile site. This version of the code should contain no frames and be mobile friendly for access from any modern smartphone or tablet running iOS, Android, or Windows. Vendor provides a sample ADA/Mobile Link.

2. Administrative Privileges. Does the application require local administrative privileges to the device it is running on? If so, please explain.

3. Application Security and Architecture. Please explain your approach to application security. For example, do you follow practices set forth by the SANS Institute, Securing Web Application Technologies <https://www.sans.org/cloud-security/securing-web-application-technologies/> and the practices of Open Web Application Security Project [www.owasp.org](http://www.owasp.org)?

4. Branding. What options do we have to add our own styles, colors, logo, wordmarks, etc.? If this is SaaS, please explain our options to brand the URL as cityofmadison.com?

5. Browser Support. Indicate the architecture used to develop the application. Indicate if all content is rendered in standard HTML5 and is viewable in all modern browsers. Please indicate any browser restrictions, including Microsoft Edge, and the preferred browser(s) and version(s) recommended for best user experience.

6. Certificates and Secure Protocols. Are there any security certificates required, such as SSL? What levels of SSL or TLS are required and minimally supported?

7. Client Footprint. Does this software require installation of anything on client workstations? If so, please explain. What are the recommended workstation requirements such as ram, storage, processing power, etc.?

8. Data Privacy. Please explain how you manage protecting Personally Identifiable Information (PII) as defined in Wis. Stat. § 19.62(5) and other confidential information in your application.

9. Identity and Permissions Management. Please describe how identity management is handled. Does the application provide for integration with the City’s Active Directory system? How are system permissions managed? Can AD groups be leveraged – please explain and be specific. Are proper controls in place to prevent direct access to the database?

10. Internet Access. For either City-hosted or SaaS solutions, are there minimum internet bandwidth requirements that end-users should have for the best user experience?

11. Legacy Data. If applicable. Please describe your method to convert data from legacy system(s).

12. Mobile Device Support. Please describe what mobile devices your application supports. Please describe what the connectivity requirements are? How does your system operate in areas without connectivity to our network or the internet?

13. Multilingual Support. Please describe the ability of your software to operate in a multilingual environment. For example, how are translations for field labels, error messages, confirmation emails, report headings, and the like handled? What languages are supported? How do users specify which language they would prefer to use? Do you accept special characters and accented characters to be entered into forms and fields?

14. Open Data. Please explain your support for Open Data Standards found at <http://project-open-data.github.io>. Do you have experience interfacing with ESRI’s Open Data portal?

15. Personalization. If this system is collecting names and other demographic information, please let us know to what level of granularity is the information collected? What flexibility does this system offer for gender identity? See the Ciy’s Gender-Inclusive Language Style Guide at <https://www.cityofmadison.com/mayor/apm/hr/APM2-52Attach2.pdf>. How do you manage name changes, gender changes, and updates to other demographic information? Can individuals manage their own profile?

16. Personal Privacy. We sometimes have individuals that qualify for keeping their information private so that even their names are excluded or redacted in public records requests. Other times we give individuals the ability to self opt-out. Please indicate how your system could handle these scenarios.

17. Records Compliance and Data Access. Please indicate how access to data will be available to comply with Wisconsin open records laws. Do we have the ability to apply retention and disposition schedules to the data within the application? If this is Software-as-a-Service, how does the City ensure all of our data is purged from your system according to the data/records retention schedule or upon contract termination? Will we have unfettered access to our data that allows us to download and store it on our premises, and will there be additional costs to access the data for these purposes? Can we use our own reporting tools such as SSRS? Does the application have published API’s and/or web services available for us to use?

18. Software Modifications. Are you willing to make software modifications?

19. Third Party Software. Fully describe any third party software that will be needed for this system, and how you manage licensing, maintenance, and support for those.

**b. Special Cases**

1. Financial Reporting and Data Sharing. Please explain your experience in providing GASB-34 compliant financial reporting and data sharing with Government oriented financial software. Do you have any experience interfacing with [Munis](https://www.tylertech.com/solutions-products/munis-product-suite)?

2. HIPAA Compliance. If this application is involved in collecting or processing protected health information, please provide proof of a HIPAA audit conducted by an independent auditor against the OCR HIPAA Audit Protocol.

3. What would your requirements be for the format of that data?

4. PCI Compliance. If this application involved collecting or processing any type of online payments or financial transactions, please provide a PCI DSS Attestation of Compliance from within the past two year, and proof of registry on the VISA Global Registry of Service Providers.

5. Spatial Data. If this application is managing or interacting with spatial data, the City of Madison used ESRI-based GIS software for managing spatial data. Please explain your experience interfacing with ESRI software.

**c. Support and Upgrades**

1. Fully explain when support is available. Include what hours are included in your maintenance agreement as well as what is available as extended service.

2. Describe your levels of severity for support calls and what your typical response times are for each level of severity.

3. Describe your handling of bugs in your software and subsequent fixes for these bugs.

4. If you allow modifications, how do you support those modifications going forward? Are they included in new releases?

5. How are new releases and enhancements developed and notification of availability made to your customers.

6. How often do you provide product upgrades, and are the costs of upgrades included in the annual maintenance?

7. Describe a typical upgrade process, including the length of time expected and if system downtime is expected.

8. Is source code provided with your software? If not fully explain what provisions are made for the source code if your company goes out of business.

9. Do you have a user group and/or an annual conference?

**d. Surveillance Technology**

Surveillance Data means any electronic data collected, captured, recorded, retained, processed, intercepted, analyzed, or shared by Surveillance Technology

Surveillance Technology means any hardware, software, electronic device, or system utilizing an electronic device, owned by the City or under contract with the City, designed, or primarily intended, to collect, retain, process, or share audio, electronic, visual, location, thermal, biometric, olfactory, or other personally identifiable information of members of the public for the purpose of surveillance. Surveillance Technology includes, but is not limited to: cell site simulators; automatic license plate readers; gunshot detection systems; facial recognition software; gait analysis software; video cameras that record audio or video and can transmit or be remotely accessed; and unmanned aircraft systems equipped with remote video capabilities. Surveillance Technology does not include: office hardware, such as TVs, computers, credit card machines, copy machines, telephones and printers; video conferencing equipment, cell phones, cameras, and video cameras not used for surveillance and operated manually; computers, software, hardware or devices used to monitor *employees* or to monitor non-public areas in city buildings; and emergency medical rescue equipment. See Madison General Ordinance Sec. 23.63(2) for a complete list of items that are not considered Surveillance Technology.

1. Will the Surveillance Data be shared with another entity? If so, is there a data sharing agreement to share the surveillance data with the other entity?

2. Will you (the vendor) be hosting the Surveillance Data? If so, please explain.

3. What access, if any, will you have to our Surveillance Data? Please explain.

# II. HOSTING

**a. Self-Hosting Requirements (Hosted by the City)**

The City may, at its option if available, choose to host the application ourselves. Please:

1. What servers are recommended? For example, do you recommend separate application, web, and database servers?

2. Minimum server requirements. Cores, storage, ram, etc.

3. Do you support VMWare environments?

4. What DBMS is recommended, and what levels and versions?

5. If MS-SQL is supported, do you support Availability Groups?

6. Will your application run under a load balancer?

7. Is network attached storage supported?

8. What would the estimated disk storage requirements be?

9. Please list all software components that the City will need to track to ensure system security, e.g., your system uses Java, .Net, C#, ColdFusion, Drupal, etc.

10. Do you have an installation and/or administrator guide? If so, please attach document(s).

**b. Hosting Data Center Criteria (Hosted by Vendor or their Designated Agent)**

The City may, at its option if available, choose to have you host this application. Please describe:

1. Antivirus Protection. Please indicate the antivirus software being used and how it is implemented.

2. Data Access. Please explain who will have access to what data, and when. Is explicit authorization required for access to our production environment? What about any data stored for your purposes, is it purged as soon as it’s no longer required?

3. Data and Application Backups. Please explain how backups of data and applications are performed and the backup policies that are in place. Please indicate your method for routinely testing your backups.

4. Data Encryption. Is data in your platform encrypted both in transit (while it’s moving between users and servers) and at rest (when it’s stored in the cloud)? Please explain your encryption protocols.

5. Data Redundancy. Please explain how data redundancy is provided.

6. Incident Response. Please describe how you classify and incident, and what your incident response plan is.

7. Internet Stability – Geographic Redundancy. Does the vendor house data in a secure SSAE 16 and PCI compliant data center? Indicate who owns and operates the data center(s). Outline the features of the datacenter, including redundant Internet providers, redundant power and cooling, and secure biometric access to the physical facility. Indicate how systems are backed up and synchronized between one or more other datacenters, and their geographic locations to provide for full geographic redundancy should one of the sites become inaccessible.

8. Logging. What types of information about my environment would be logged, and how long are logs available? Please explain your logging protocols.

9. Penetration Tests. Penetration tests, also known as pen tests, are simulated attacks on a system. They are performed by authorized experts to evaluate that system’s security and identify vulnerabilities, making them an important component of a proactive cybersecurity strategy. Please describe how often you perform pen tests.

10. Separation of Systems. Please describe how your environment provides for separation of instances so that corruption of one instance or client will not affect the City of Madison. Please describe your practices to keep production environments isolated from test and development.

11. Server and Software Patching. Please provide your policy or documentation that shows the methods you use to ensure your hardware and software remains patched and up-to-date.

12. Data Center Certifications. Please provide documentation that shows the data centers used to support this application meet the following certifications:

**SSAE 18**

The Statement on Standards for Attestation Engagements No. 18, establish requirements and provide application guidance to auditors for performing and reporting on examination, review, and agreed-upon procedures engagements, including Service Organization Controls (SOC) attestations.

* Type 1 – A data center’s description and assertion of controls, as reported by the company.
* Type 2 – Auditors test the accuracy of the controls and the implementation and effectiveness of controls over a specified period of time.

**SOC 1**

This set of Service Organization Controls reports, developed by the AICPA, measures the controls of a data center as relevant to financial reporting.

**SOC 2**

This report and audit is completely different from the previous. SOC 2 measures controls specifically related to IT and data center service providers. The five controls are security, availability, processing integrity (ensuring system accuracy, completion and authorization), confidentiality and privacy. There are two types:

* Type 1 – A data center’s system and suitability of its design of controls, as reported by the company.
* Type 2 – Includes everything in Type 1, with the addition of verification of an auditor's opinion on the operating effectiveness of the controls.

**SOC 3**

This report includes the auditor’s opinion of SOC 2 components with an additional seal of approval to be used on websites and other documents. The report is less detailed and technical than a SOC 2 report.

# III. TERMS AND CONDITIONS

a. Fully describe licensing terms and conditions and how licenses are structured (e.g. named user, concurrent users, etc.). Attach a copy of any required licensing agreements or EULAs. Please also describe your licensing model – e.g. perpetual, subscription based, named users, concurrent users, etc.

b. Fully describe terms and conditions of your software support/maintenance program. Please include a copy of your standard agreement(s) for support and maintenance.

# IV. TRAINING

a. Fully describe all training that your company will provide, include the following information.

1. End user training; class size, length of class.

2. System administration training; class size, length of class.

3. Application support training.

4. Any custom reports tools training.

5. Any other training you deem necessary for use of your software.

b. Explain where the training is to be held, and who will be providing it.

c. Do you have any online training courses available? If yes, fully describe what is available.