ITS Cloud Solution Questionnaire

Document ID	NA
Effective Date	1/1/2025
Owner	Metro ITS CISO
Info Classification	Public Information
Page No.	Page 1 of 7

AUDIENCE

All Metropolitan Government (Metro) employees, contractors, and third-party users.

PURPOSE

The goal of this questionnaire is to provide various divisions within Metro ITS the necessary information to support cloud based or hosted solutions. These solutions include production, backup, and proof of concept implementations. It is vital to provide all information to ensure a smooth and efficient implementation. Completion of this questionnaire should be done as early as possible in the project process and must be completed prior to any phone call with ITS resources.

It is vital that Metro Departments and Agencies make pragmatic decisions about where and when to use cloud based or hosted solutions. Metro Departments and Agencies are ultimately responsible for working with their vendors to ensure solutions are secure - from design, implementation, and production phases of the project. It is strongly recommended that Metro Departments and Agencies review Metro's *IT Guidance – Cloud Solution Considerations* when researching cloud-based solutions. Metro ITS strongly recommends completion of Metro's *IT Guidance – Application Checklist* to ensure secure and healthy deployment of a solution, especially if that solution supports critical service.

Vendors proposing cloud hosted solutions should understand and be expected to agree to the following requirements. Exceptions can be made, depending upon risk to Metro and the applicability of the requirement.

1. Metro retains full control and ownership of all data.
2. All data including back-ups must reside and be hosted within the US jurisdiction.
3. Solution should be able to utilize Metro's identity management infrastructure. These solutions include AD FS and Entra ID with support for all modern authentication protocols.
4. Solution must use and require Multi-Factor Authentication. This includes vendor access to backend infrastructure.
5. All authentications should be logged, including source IP.
6. Audit logs of data access or configuration changes must be made available to Metro upon request within 72 hours or 24 hours in case of confirmed security incident.
7. Identified Metro contact must be notified of all critical vulnerabilities with the solution utilizing the Common Vulnerability Scoring System (CVSS) for vulnerabilities scored higher than 7.
8. If hosted solution will contain any sensitive data or must meet any regulatory requirements as determined by the owning department, certifications and accreditation or third-party attestations of security program must be provided for review to ensure adequate security is in place.

9. Solution must utilize the principle of least privilege when integrating into other Metro solutions with permissions documented and provided for review.
10. If the solution will contain a public facing website, the URL may need to be registered with a .gov suffix.

QUESTIONS

1. Is this a "Proof-Of-Concept" installation? If so, how long will the Proof-of-Concept run and when does it need to be in place?

2. What is the name and version of the solution in use?

3. Who is the vendor for the solution? Is there an existing contract with the vendor?

4. When is implementation scheduled to occur?

5. Who will be the Metro Departments and Agencies staff member that is the solution point of contact and what is their phone number and email address?

6. Who is the customer for this solution (internal users, public, both)?

7. What is the criticality of the service this application provides/supports (How important is availability of this application to your business)? Criticality classifications are found in **Appendix A.**

8. What is the classification of any data transferred/stored in use of this service? Metro's information classification policy is located here. A list of examples of sensitive information is found in **Appendix B**.

9. Does Metro retain full control and ownership of all data generated by this solution?

10. Is data generated by this solution transmitted to any third-party – raw, aggregated, or anonymized?

11. Will this solution use a private network connection, such as AT&T Netbond, or will all traffic go across the public internet?

12. EXACTLY what network traffic will be required for this solution? The department and agency must provide complete network communication information showing ALL network traffic that must be allowed to make this solution work. That information includes IP address ranges, protocols, ports, direction, or traffic, etc. The solution provider should be able to give this information to the Metro Department and Agency in a clear, easy to understand format that reflects ONLY what network traffic is needed.

13. Has any analysis been completed on the amount of data that will traverse the Metro network and use Metro's network pipe? In other words, what is the load on the network? This should include times when load might be high, such as any backups to the hosted solution from the Metro network.

14. If backups or any large data transfers traversing the Metro network will occur, are those scheduled for a specific time? What is the expected average size of these transfers?

15. Does the data that will be moving to the cloud fall under any compliance-related regulations or requirements? This includes data such as Personally Identifiable Information (PII), Personal Health Information (PHI), payment card data (PCI-DSS), etc. If so, which ones?

16. Has the provider verified that all data, including backups, are hosted within US jurisdiction?

17. Has the provider given proof of any third-party attestations or certifications of the provider's security? Examples include FISMA, CSA STAR Certification, etc. Does the provider meet compliance requirements to SSAE 16/SAS70-II, SOX, PCI-DSS, ISAE3402, SOC1, 2 or 3, Safe Harbor, or other regulatory certification requirements that attest to the information security practices within the provider?

18. Are data in transit and file uploads or transfers using current, secure encryption protocols? For data in transit Cloud providers should be using SSL from an established, reliable, and secure independent CA. The SSL CA needs its authentication practices audited annually by a trusted third-party auditor. SSL should deliver at minimum 128-bit encryption and optimally 256-bit encryption based on the new 2048-bit global root.

19. What encryption technology is utilized for data storage, if applicable?

20. Will this solution use a standalone credentials or will it be using Metro's identity management infrastructure (Active Directory, ADFS, etc.)? If the intent is to use Metro's network credentials, the solution provider must provide documentation on how that is facilitated.

21. Does the solution provide support for two-factor authentication?

22. Is any part of the system physically accessible by the public or outside (non-Metro) agencies? Examples include kiosks and public computer terminals.

23. Does this solution support separate systems for any Internet or public-facing access? Metro ITS requires any public-facing system be installed in our "DMZ network", with only back-office systems residing within the internal network.

24. Does this solution use any technology or software solution that allows direct Internet access for maintenance or management? Examples include Teamviewer and VNC.

25. What is the vendor notification process after discovering a critical vulnerability or incident affecting this application?

26. For critical applications hosted in the cloud, is denial-of-service protection included?

27. For Internet-facing web applications, is a web application firewall (WAF) included?

28. Does the solution have the capability to audit access of the data or settings of the application? If so, how long are those records or logs kept and who can access or request the logs?

29. For any Infrastructure as a Service (IaaS) or Platform as a Service (PaaS) solution, does the cloud platform provide a near real-time cost monitoring dashboard or mechanism to report cloud spend? Does the solution provide mechanisms to apply business logic to the cost data in order to align results to rate model/chargeback activities? The solution provider should be able to give this information to the Metro Department and Agency in a clear, easy to understand format.

Appendix A

Business Impact Analysis – Criticality Level Standard

Criticality Level	**Failures or outage in this class can result in:**
Mission Critical MTD*: 0 – 4 hours	Any outage results in immediate cessation of a primary function, equivalent to major impact to brand name, customer satisfaction or safety across multiple departments. Service(s) that are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. • Widespread business stoppage with significant impact • Risk to human health/environment • Public, wide-spread damage to organization's reputation • Significant employee productivity degradation across multiple departments
Business Critical MTD*: 4 hours	Any outage results in immediate cessation of a primary function, equivalent to major impact to brand name, customer satisfaction or safety across a department. Services that are critical to public health or safety and must be protected by a vital plan that would allow resumption of operations within a very short timeframe. • Localized business stoppage with significant impact • Public, wide-spread damage to department's reputation • Significant employee productivity degradation within a department
Business Essential MTD*: 4 hours – 24 hours	Significant impact to business processes. Service(s) are required to administer functions that need to be performed. Business can continue operations in these areas within a certain period until the service can be restored. • Direct revenue impact • Direct negative customer satisfaction • Compliance violation • Non-public damage to organization's reputation • Moderate employee productivity degradation
Business Important MTD*: 1 days – 3 days	Minor impact to business processes. Service(s) are necessary but short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of citizens. • Indirect revenue impact • Indirect negative customer satisfaction • Minimal employee productivity degradation
Non Critical MTD*: 7 days +	Low to no impact to business processes. Service(s) are not necessary, and short-term interruption or unavailability is acceptable. They do not play any role in the scheme of the health, security, or safety of citizens. • No revenue impact • No negative customer satisfaction • Minimal employee productivity degradation
Terms	*Maximum Tolerable Downtime (MTD) is the maximum length of time the application can be down without causing unacceptable consequences to the department.

Appendix B

Sensitive Information Checklist

Below are various types of “Sensitive Information”, which is any information, classified as "Confidential" or "Restrictive" as defined by the *Metropolitan Government Information Classification Policy*. This list is not all inclusive, but meant to provide examples. Metro departments are responsible for assigning data classification based on any applicable regulations, etc.

TYPES:

ð Social Security Numbers

ð Protected health information, including medical records of patients

ð Credit card numbers and any related personal identification numbers or authorization codes

ð Records of students in public educational institutions

ð Investigative reports

ð Criminal Justice Information

ð Criminal History Record Information

ð Attorney/client privilege

ð Bank account information, including routing and account numbers

ð Standard Operating Procedures including, but not limited to:

- o All riot, escape and emergency transport plans
- o All contingency plans of a governmental entity prepared to respond to or prevent any violent incident, bomb threat, ongoing act of violence at a school or business, ongoing act of violence at a place of public gathering, threat involving a weapon of mass destruction, or terrorist incident.
- o Information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.

ð Residential street address, home telephone and personal cell phone numbers of public employees

ð Proposals received in response to a request for service prior to the completion of evaluation for service

ð Information that would allow a person to obtain unauthorized access to confidential information or to government property

ð Plans, security codes, passwords, combinations, or computer programs used to protect electronic information and government property

ð Information that would identify those areas of structural or operational vulnerability that would permit unlawful disruption to, or interference with, the services provided by a governmental entity

ð Information and records that are directly related to the security of any government building, including, but not limited to,

- o Information and records about alarm and security systems used at the government building
- o Security plans, including security-related contingency planning and emergency response plans
- o Blueprints and information about building infrastructure (water, electrical, network, etc.)

Appendix C

Sample diagram of an application infrastructure. Ideally, the communications paths should be documented with ports used, etc.