Metro Information Security Agreement (ISA) Part 1: Questionnaire

Purpose

The purpose of this Metropolitan Government's (Metro) Information Security Agreement Questionnaire is to identify contractual requirements between Metro and an entity who desires to do one or more of the following:

- Provide software or hardware to Metro;
- Connect to the Metro network;
- Provide services over a network (i.e., cloud-bases services, etc.); or
- Access or store Metropolitan Government department or agency data.

Your responses will be used to craft appropriate information security contractual language (Part 2). The representative of the Contractor responding to this questionnaire must sign at the bottom of the questionnaire.

Definitions

Contractor – Non-Metro Government organization or individual.

Sensitive Information – Any information classified as "Confidential" or "Restrictive" as defined by the Metropolitan Government Information Classification Policy (see https://www.nashville.gov/sites/default/files/2022-11/ISM7_InformationClassificationPolicy.pdf?ct=1669737691). The classification of the data that a Contractor is given access to should be determined by and communicated to the Contractor by the department that is the customer for this contract. **A list of data that Metro has classified as "Sensitive" is attached in Appendix A.**

Questions

For any questions regarding this document, please contact CISO@nashville.gov.

Name of Responding Company:_____

Name of Responding Person: _____ Phone:_____

Question	Response
1. Will Contractor provide, license, or sell software or computer related hardware that will reside on systems, workstations, or devices on the Metro Government network or as a component of the Metro Government IT Infrastructure?	☐ Yes ☐ No
If **Yes**, please describe the Products or Services:	
2. Will Contractor have access to or collecting on behalf of the Metropolitan Government any Sensitive Information? Please refer to **Appendix A** for a list of some, but not all, data currently classified as "Sensitive".	☐ Yes ☐ No
If **Yes**, please describe the type of data:	
3. Will Contractor need **temporary** administrative access to install, configure, implement, update and/or upgrade applications or systems?	☐ Yes ☐ No
4. Will Contractor require **ongoing** administrative access in order to support applications or systems on the Metro Government network or Metro Government Infrastructure?	☐ Yes ☐ No
If **Yes**, please describe the necessity for continued administrative access:	
5. Will Contractor need network access from an external network to the Metro Government network using a remote access technology?	☐ Yes ☐ No
6. Will Contractor need a **dedicated or perpetual** network connection to Metro Government network (e.g., via Permanent VPN, B2B VPN)?	☐ Yes ☐ No
7. Will Contractor provide electronic media cleansing, data or data storage media/device destruction service for Metro Government?	☐ Yes ☐ No
If **Yes**, please provide internal procedures ensuring successful destruction:	
8. Will Contractor providing services that involves use or disclosure of public health information and Contractor is not already considered a Covered Entity, per 45 CFR 160.103 definition of Business Associate?	☐ Yes ☐ No

9. Will Contractor providing or implementing an application or system which will accept as input, store, transmit or process Cardholder Data; providing Services which involve credit card PIN pad devices; and/or providing application or system development for systems which will store, transmit, or process Cardholder Data on behalf of Metro Government?	☐ Yes ☐ No
10: Will Contractor storing any data owned by Metro Government using cloud storage, either stored by the Contractor or using a third party hosted solution, such as Dropbox, Box, Google Docs, Amazon Web Services, Microsoft Azure etc.?	☐ Yes ☐ No
If **Yes**, what are the Products or Services to be provided?	
11: Will Contractor develop software, including mobile applications, or create customizations for software that will be used by Metro Government?	☐ Yes ☐ No
12: Is the Contractor proposing a hosted solution (IaaS, PaaS, SaaS)?	☐ Yes ☐ No
13: Will Contractor provide a standalone Artificial Intelligence (AI) solution, or a solution embedded with or using AI within its software or service offering?	☐ Yes ☐ No
If **Yes**, please describe how AI is used and provide link to Contractor's responsible AI strategy, policy, etc.	

Signature of Responding Person: _____

Appendix A. 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*.

Please indicate if a Contractor will be providing a service or solution that will use as an input or output, store, process or have any access to any of the information below, in any form, by checking the box next to the data type.

TYPES:

- ☐ Social Security Numbers
- ☐ Protected health information, including medical records of patients
- ☐ Credit card numbers and any related personal identification numbers or authorization codes
- ☐ Records of students in public educational institutions
- ☐ Investigative reports
- ☐ Criminal Justice Information
- ☐ Criminal History Record Information
- ☐ Attorney/client privilege
- ☐ Bank account information, including routing and account numbers
- ☐ Standard Operating Procedures including, but not limited to:
    - All riot, escape and emergency transport plans
    - 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.
    - Information that could be used to disrupt, interfere with, or gain unauthorized access to electronic information or government property.
- ☐ Residential street address, home telephone and personal cell phone numbers of public employees
- ☐ Proposals received in response to a request for service prior to the completion of evaluation for service
- ☐ Information that would allow a person to obtain unauthorized access to confidential information or to government property
- ☐ Plans, security codes, passwords, combinations, or computer programs used to protect electronic information and government property
- ☐ 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
- ☐ Information and records that are directly related to the security of any government building, including, but not limited to,
    - Information and records about alarm and security systems used at the government building
    - Security plans, including security-related contingency planning and emergency response plans
    - Blueprints and information about building infrastructure (water, electrical, network, etc.)
- ☐ OTHER _____

If you have any questions about this checklist, please contact the department contact for this contract.