Sensitive Information and Data Access Terms – Annex
(Last updated – September 28, 2025)

1. SENSITIVE INFORMATION / DATA SECURITY

(a) The Contractor must protect, and take measures to assure that its subcontractors at each tier protect, "**sensitive information**" made available during the course of a WMATA contract or subcontract in accordance with 49 U.S.C. § 40119 (b) and implementing DOT regulations, "**Protection of Sensitive Security Information**," 49 C.F.R. Part 15, and with 49 U.S.C. § 114(s) and implementing Department of Homeland Security regulations, "Protection of Sensitive Security Information," 49 C.F.R. Part 1520.

(b) Each party, to the extent permitted by law and regulation, will safeguard and treat information obtained pursuant to the other party's disclosure as confidential where the information has been marked "confidential" or "proprietary" by the disclosing party. Subject to the foregoing and to the extent permitted by law and regulation, WMATA will not release to the public, any such confidential information of Contractor, pursuant to a Public Access to Records request, without prior notification to Contractor.

(c) Any and all personally identifiable information regarding WMATA's customers and including, without limitation, existing, past and potential customers, shall be considered "**WMATA's Customer Information**." Contractor will refrain from using, disclosing, reproducing, summarizing and/or distributing WMATA's Customer Information except for purposes expressly authorized by this Contract. Without limiting Contractor's obligations herein, any collection, maintenance, and/or use of WMATA's Customer Information by Contractor shall be undertaken (i) subject to the then current documented privacy policies of WMATA and, in all cases (ii) in compliance with any applicable laws governing WMATA's collection, maintenance, transmission, dissemination, use and destruction thereof. Upon reasonable request from WMATA, Contractor shall provide access to WMATA and/or its designates, and the right to inspect, all Records (as defined under Section 13 of the Standard IT Terms and Conditions) relating to the collection, processing or transfers of data relating to WMATA's Customer Information at each location at which any of such information may be stored, accessed or processed. Contractor agrees to cooperate in any regulatory investigation or in any internal investigation by WMATA, and in responding to any inquiry by any customer of WMATA relating to such customer's personal information.

(d) Contractor shall and shall ensure its Personnel, to the extent applicable, provide the Products and perform all Services in strict compliance will all WMATA policies and procedures relating to local and remote network access and connectivity, which policies and procedures shall be made readily available to Contractor upon request.

(e) Contractor shall, to the extent applicable, adhere to the security policies and standards set forth in this Contract, its attachments and the security policies and procedures provided to Contractor in advance, which security may be updated from time to time, and ensure that its Personnel adhere to all such security policies and standards.

(f) Contractor shall conduct annual assessments of the risks to the security of WMATA's Customer Information acquired or maintained by Contractor or its Personnel in connection with the Products and Services. Contractor's obligations will include the following:

i. mandatory cyber training for all relevant Personnel, including as necessary to implement and comply with all relevant security policies and procedures;

ii. identification of internal and external threats that could result in unauthorized, alteration, or destruction of WMATA’s Customer Information and systems used by WMATA; and

iii. qualitative assessment of the likelihood and potential damage of such threats, taking into account the sensitivity of WMATA’s Customer Information. Contractor shall test key controls, systems, and procedures relating to information security on a regular basis. Contractor shall determine the appropriate frequency and nature of such tests based on good industry practice regarding network and system security and the procedures it takes to safeguard its own proprietary and commercially sensitive information. Contractor shall maintain appropriate documentation describing its information security program, and will provide such documentation to WMATA upon request.

2. NON-DISCLOSURE AND DATA ACCESS

This clause sets forth the Contractor’s obligations regarding Contractor’s access to and use of WMATA’s proprietary, confidential, or personally identifiable information (PII) in order to carry out the requirements of this Contract. WMATA will provide such information in accordance with this clause. Unless otherwise identified, all terms defined within this Annex apply only to those terms as they appear herein. If similar terms appear within this Contract, such terms shall have the meaning assigned to them in that context.

A. Definitions.

1. “**Confidential Information**” shall mean any non-public, proprietary, or otherwise protected data, information, documents or other material, whether in tangible or intangible form, in whatever medium, provided or disclosed by a party to the other party that is designated as confidential or similarly marked, or that would reasonably be deemed to be the sensitive or confidential information of the disclosing party in light of the context of the information or circumstances of disclosure, and may include, without limitation: (i) any marketing strategies, plans, financial information, or projections, costs, operations, sales estimates, business plans or business process information, and business performance results relating to the past, present or future business activities of such party, its affiliates, subsidiaries and affiliated entities; (ii) plans for development, engineering, or manufacturing of products or services, and customers or suppliers; (iii) any scientific or technical information, invention, design, process, procedure, formula, improvement, technology or method; (iv) any concepts, reports, data, research, know-how, works-in-progress, designs, development tools, specifications, computer software, source code, object code, flow charts, databases, inventions, information and trade secrets; (v) any screening, applicant, or pre-employment assessments, surveys, or other testing; (vi) any customer data; (vii) any other information that may reasonably be recognized as confidential information whether or not designated as such; and (viii) any copies or portions of documents prepared by or for the receiving party, or information generated by the receiving party or by its representatives that contains, reflects, or is derived from any of the foregoing. Any information received orally shall be treated as Confidential Information if the disclosing party identified the information as confidential or proprietary prior to its disclosure or if the information orally disclosed would be understood by a reasonable person to be confidential. The existence of this clause and the discussions between the parties with respect to the purposes hereof and the status of such discussions shall also be considered confidential and shall be subject to the nondisclosure obligations set forth in this clause.

2. “**Personal Information**” means public or non-public information provided or transmitted to Contractor by WMATA, or to which access was provided to Contractor by WMATA, or that Contractor receives on WMATA’s behalf, that identifies or can be used to identify an individual, either alone or in combination with other information or is otherwise designated as Personal Information by applicable law.

3. “**Protected Information**” means Confidential Information and Personal Information.

4. “**Security Incident**” means any act or omission that actually or potentially compromises either the security, confidentiality, integrity or availability of Protected Information or the Security Standards put in place by Contractor that relate to the protection of the security, confidentiality, integrity or availability of Protected Information. A Security Incident includes any inadvertent or unauthorized use, loss, alteration, access, copying or disclosure of any of the Protected Information.

5. “**Security Standards**” means industry standard security features in all physical, technical, administrative and organizational safeguards that Contractor uses to access, store, process and/or transmit the Protected Information, in alignment with ISO/IEC 27001, as that standard or its successor standards may be amended. It also includes any requirements mandated by WMATA’s Office of Cybersecurity.

B. Confidentiality and Non-Use.

Contractor shall have the right to refuse to accept any Protected Information under the Contract prior to disclosure. Protected Information disclosed despite such a refusal shall nonetheless be covered by the confidentiality obligations under this clause. As a condition of WMATA’s disclosure of Protected Information, Contractor shall, and, if applicable, cause Contractor’s Personnel to access, store, process and/or transmit Protected Information solely within the United States, at all times. In addition, Contractor shall require that any of its Personnel accessing, storing, processing and/or transmitting Protected Information reside and work within the continental United States at all times. Contractor shall restrict the storage of Protected Information to servers, workstations, networks or any other device of any kind physically located within the continental United States. Upon receipt of Protected Information, Contractor shall and, if applicable, cause its Personnel to:

i. Use the highest degree of care to keep Protected Information strictly confidential and not disclose to persons or entities other than Contractor or its Personnel who have a reasonable need to know such Protected Information in connection with the permitted purposes hereunder and who have executed a non-disclosure agreement with terms no less stringent than these this clause. Contractor will be liable for its Personnels’ unauthorized use and/or disclosure whether caused by negligence or otherwise;

ii. Use such Protected Information solely and exclusively for the limited purposes described herein and for no other purposes whatsoever, except with the prior written consent of the CO; and

iii. Use the highest degree of care to protect Personal Information at all times in strict compliance with all applicable laws and current Security Standards in order to prevent any unauthorized use, including disclosure, loss or alteration. Within thirty (30) days of a written request from WMATA or termination, Contractor shall and shall cause all of its Personnel to, at WMATA’s option, either: (i) return the Protected Information to WMATA; or (ii) destroy the Protected Information pursuant to the media sanitization guidelines set forth in National Institute of Standards and Technology (NIST) special publications (SP) to include SP 800-88 Rev. 1 as these guidelines or successor guidelines may be amended and provide WMATA with a certificate signed by an officer of Contractor stating that such destruction has occurred.

C. Exceptions to the Confidentiality and Non-Use Obligations (Applicable Only to Confidential Information).

The obligations imposed by subclause B above shall not apply, or shall cease to apply, to Confidential Information if or when, and to the extent that, such Confidential Information:

i. is or becomes lawfully available to the public or within the public domain other than as a result of Contractor's disclosure in violation of these this clause or due to some other unlawful disclosure by an unrelated third party; or

ii. was lawfully in Contractor's possession prior to receipt from WMATA whether before or after the date of this Contract; or

iii. is received by Contractor independently from a third party free to lawfully disclose such information to Contractor; or

iv. is subsequently developed independently by Contractor; or is approved in writing by WMATA for disclosure or use.

It shall not be a breach of this Annex for Contractor to disclose Confidential Information when and to the extent that such disclosure is required by law or applicable legal process, provided that Contractor in making such disclosure shall: (i) give WMATA as much prior notice thereof as is reasonably practicable so that WMATA may seek such protective orders or other confidentiality protection as it, in its sole discretion and at its sole expense, it may elect; and (ii) reasonably cooperate with WMATA to protect the confidential or proprietary nature of the Confidential Information that must be disclosed. For the sake of clarity, none of the above exceptions shall apply to Personal Information that must be protected from inadvertent or unauthorized disclosure at all times.

D. Inadvertent or Unauthorized Disclosure; Security Incidents.

Contractor shall comply with all applicable laws that require the notification of individuals in the event of a Security Incident, or other incident requiring notification. In the event of a Security Incident, or other incident requiring notification under applicable law, Contractor agrees to:

i. Notify WMATA by telephone and e-mail of such an event within 48 hours of discovery.

ii. Assume responsibility for informing all such individuals in accordance with applicable law, and

iii. In addition to its indemnification obligations in Section 26 of the Standard IT Terms and Conditions or elsewhere in the Contract, indemnify, hold harmless and defend WMATA and its stakeholders, officers, and employees from and against any claims, damages, or other harm related to Security Incidents.

If Contractor becomes aware that Protected Information may have been accessed, disclosed, acquired or lost without proper authorization and contrary to the terms of this Annex or the

Contract, then the Contractor shall immediately take such actions as may be necessary to preserve forensic evidence and eliminate the cause of the Security Incident. Contractor shall give highest priority to immediately correcting any Security Incident and shall devote such resources as may be required to accomplish that goal. Contractor shall provide WMATA information necessary to enable WMATA to fully understand the nature and scope of the Security Incident.

E. No Creation or Transfer of Rights in Protected Information or Intellectual Property.

Nothing in this clause shall obligate WMATA to make any particular disclosure nor to give Contractor any rights, title, license or interest whatsoever in or to the Protected Information or in or to any existing or future patents, know-how, inventions, trademarks, copyrights or other intellectual property of WMATA.

F. No Representations or Warranties.

UNLESS MADE BY WMATA IN WRITING, ALL REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO PROTECTED INFORMATION, WHETHER EXPRESS OR IMPLIED, ARE DISCLAIMED.

G. Indemnification.

Contractor shall indemnify, defend and hold WMATA its stakeholders, officers, and employees harmless from all claims, liabilities, damages, or judgments involving a third party, including WMATA’s costs and attorney fees, arising out of or in connection with Contractor’s failure to meet any of its obligations under these this Annex, including but not limited to Contractor’s obligations to safeguard Protected Information from Security Incidents.

H. Duration of Obligations.

The Contractor’s obligations under this Annex shall continue in full force and effect and be coterminous with the Contract. However, the obligations protect, not to use or disclose, and to return on request or destroy Protected Information already disclosed to the Contractor at the time of termination shall continue for as long as Contractor holds the Protected Information.

I. Survival

Each party’s obligations under this Annex which are not, by the express terms of this Annex, fully to be performed during the term of the Contract, shall survive the expiration or termination of the Contract for any reason.