SECTION A-1

General Terms and Conditions

1 **Safeguards.** In addition to the controls specified in the exhibits to this Agreement, Contractor agrees to implement administrative, physical, and technical safeguards to protect the availability, confidentiality and integrity of Metropolitan Government of Nashville and Davison County (Metro Government) Information, information technology assets and services. All such safeguards shall be in accordance with industry-wide best security practices and commensurate with the importance of the information being protected, but in no event less protective than those safeguards that Contractor uses to protect its own information or information of similar importance, or is required by applicable federal or state law.

2 **Inventory.** Contractor agrees to maintain at all times during the Term of this Agreement a Product and Service Inventory. Contractor shall upon request of Metro Government, which shall be no more frequently than semi-annually, provide the current Product and Service Inventory to Metro Government within thirty (30) days of the request. This Inventory reflects all products and services the Contractor offers under this Agreement, including, but not limited to, any currently consumed by Metro Government. The form of this inventory can be a link to a site, if appropriate.

3 **Connection of Systems or Devices to the Metro Government Network.** Contractor shall not place any systems or devices on the Metro Government Network without the prior written permission of the Director of ITS, designee, or the designated Metro Government contact for this Agreement.

4 **Access Removal.** If granted access to Metro Government Network or systems, Contractor and its Agents shall only access those systems, applications or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass security controls. Notwithstanding anything to the contrary in the Purchasing Agreement or other agreement between Metro Government and Contractor, Metro Government at its sole discretion, may refuse granting access right to Metro Government Network or Sensitive Information to any Agent of Contractor, and may at any time remove access rights (whether physical premise access or system access) from Contractor or any Agents, without prior notice or liability to Contractor, if Metro Government reasonably suspects a security violation by Contractor or such Agent or otherwise deems such action appropriate to protect Metro Government Infrastructure, Metro Government Network or Metro Government Information.

5 **Subcontracting/Outsourcing.**

   5.1 **Prior Approval.** Without Metro Government's prior written consent, Contractor may not subcontract with a third party to perform any of its obligations to Metro Government which involves access to Metro Government Information or connection to Metro Government Network. Nor shall Contractor outsource any Contractor infrastructure (physical or virtual) which Stores Sensitive Information without such consent. To obtain Metro Government's consent, Contractor shall contact the Metro Government ITS department. In addition, Metro Government may withdraw any prior consent if Metro Government reasonably suspect a violation by the subcontractor or outsource provider of this Agreement, or otherwise deems such withdraw necessary or appropriate to protect Metro Government Network, Metro Government Infrastructure or Metro Government Information.

   5.2 **Subcontractor Confidentiality.**   Contractor Agents are bound by the same confidentiality obligations set forth in this Agreement. Contractor or its Agent may not transfer, provide access to or otherwise make available Metro Government Information to any individual or entity outside of the United States (even within its own organization) without the prior written consent of Metro Government. To obtain such consent, Contractor shall send Metro Government a notice detailing the type of information to be disclosed, the purpose of the disclosure, the recipient's identification and location, and other information required by Metro Government.

   5.3 **Contractor Responsibility.**   Prior to subcontracting or outsourcing any Contractor's obligations to Metro Government, Contractor shall enter into a binding agreement with its subcontractor or outsource service provider ("Third Party Agreement") which (a) prohibits such third party to further subcontract any of its obligations, (b) contains provisions no less protective to Metro Government Network, Metro Government Infrastructure and/or Metro Government Information than those in this Agreement, and (c) expressly provides Metro Government the right to audit such subcontractor or outsource service provider to the same extent that Metro Government may audit Contractor under this Agreement. Contractor warrants that the Third Party Agreement will be enforceable by Metro Government in the U.S. against the subcontractor or outsource

provider (e.g., as an intended third party beneficiary under the Third Party Agreement). Without limiting any other rights of Metro Government in this Agreement, Contractor remains fully responsible and liable for the acts or omissions of its Agents. In the event of an unauthorized disclosure or use of Sensitive Information by its Agent, Contractor shall, at its own expense, provide assistance and cooperate fully with Metro Government to mitigate the damages to Metro Government and prevent further use or disclosure.

6   **Technological Errors and Omissions Insurance.** Contractor will carry Technological Errors and Omissions Liability insurance in the amount of one million ($1,000,000.00) dollars. This is in addition to any other insurance requirement identified.

7   **Additional Cyber Liability Insurance.** Contractor will carry an additional four million ($4,000,000) dollars of Cyber Liability insurance if they collect, store, and/or process any Metro Government Information that has not been specifically classified as public information by Metro.

SECTION A-2

Definitions

Capitalized terms used in the Agreement shall have the meanings set forth in this Exhibit A-2 or in the *Metropolitan Government Information Security Glossary*, which can be found on the Metropolitan Government of Nashville website . Terms not defined in this Exhibit A-2 or otherwise in the Agreement shall have standard industry meanings.

1. "Affiliates" as applied to any particular entity, means those entities, businesses, and facilities that are controlled by, controlling, or under common control with a stated entity, as well as (with respect to Metro Government) any entity to which Metro Government and/or any of the foregoing provides information processing services.

2. "Agent" means any subcontractor, independent contractor, officer, director, employee, consultant or other representative of Contractor, whether under oral or written agreement, whether an individual or entity.

3. "Agreement" means this Information Security Agreement, including all applicable exhibits, addendums, and attachments.

4. "Information Breach" means any actual or suspected unauthorized disclosure or use of, or access to, Metro Government Information, or actual or suspected loss of Metro Government Information.

5. "Effective Date" means the date first set forth on page 1 of the Agreement.

6. "Metro Government Information" means an instance of an information type belonging to Metro Government. Any communication or representation of knowledge, such as facts, information, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual, owned by or entrusted to Metro Government.

7. "Metro Government Infrastructure" means any information technology system, virtual or physical, which is owned, controlled, leased, or rented by Metro Government, either residing on or outside of the Metro Government Network. Metro Government Infrastructure includes infrastructure obtained from an IAAS provider or systems that are provided and located on the Metro Government Network as part of a Service.

8. "Metro Government Network" means any Wide Area Network (WAN) or Local Area Network (LAN) owned, operated, managed or controlled by Metro Government.

9. "Term" means the period during which this Agreement is in effect.

10. "Security Incident" means an occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of an information system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

<div align="center">**SECTION AI**</div>

<div align="center">**Artificial Intelligence**</div>

1. **Responsible Artificial Intelligence (AI) Strategy**.

   Contractor shall provide Metro Government its strategy for ensuring responsible AI. That strategy should address the following areas:

   - Soundness: Comprehend context as well as uphold data quality and model performance.
   - Fairness: Identify and remove discrimination and support diversity and inclusion.
   - Transparency: Provide explainability, understandability and traceability.
   - Accountability: Manage oversight, redress and auditability.
   - Robustness: Ensure security and resilience of systems from breaches or tampering as well as readiness of a response plan.
   - Privacy: Safeguard personally identifiable information, data ethics and human rights as well as comply with data owner consents.
   - Legality: Ensure that the intellectual property rights of third parties are respected by the use of the AI in question.
   - Sustainability: Consideration of human-centered ethics as well as societal and environmental well-being.

   This strategy shall be maintained throughout the life of the contract. Any revisions shall be communicated to Metro Government.

2. **Information Security and Privacy.**

   2.1. Contractor shall implement robust information security measures to protect all information utilized for the AI based solution, including but not limited to personal, confidential, or sensitive information. Contractor shall adhere to applicable information protection laws and regulations.

   2.2. Information sharing and access shall be restricted to authorized personnel only, and data shall not be used for purposes other than those explicitly defined in the contract. This includes training of AI solutions for other customers.

   2.3. Contractor shall follow industry standards, such as the NIST AI Risk Management Framework, for protecting all components of the AI based solution, including any algorithms, model and training data.

   2.4. Contractor shall provide a method for accessing and exporting any Metro Government information stored in and processed by the AI solution and for secure deletion of Metro Government information from the AI solution.

3. **Algorithm Transparency and Explainability.**

   3.1. Contractor shall provide clear explanations or provide guidance for interpretation of the AI algorithms and models used in the solution, enabling Metro Government to understand the decision-making process, in so much as it does not reveal proprietary secrets.

   3.2. Contractor shall maintain transparency in the sources of data used for training and shall communicate the potential biases that may arise, shall ensure that its use of these sources is consistent with intellectual property law, and shall indemnify Metro Government and hold it harmless in response to any third-party claims received regarding its use of sources of data.

   3.3. Contractor shall fully retain ownership of the AI technology or is using a solution to which they are fully licensed. If Contract is licensing AI technology, then they will retain licensing for the solution used at the time of contract signing for the duration of the contract.

   3.4. Contractor shall ensure that conversational solutions, including, but not limited to, those providing speech generation, shall be capable of identifying as being nonhuman.

4. **Ethical Considerations.**

   4.1. Contractor shall ensure that the AI solution operates in accordance with ethical guidelines, avoiding discriminatory or biased outcomes.

4.2. The AI solution shall not engage in actions that infringe upon user privacy, generate harmful content, or violate any intellectual property laws or any legal or ethical standards.

4.3. Contractor shall provide training model datasets that use bias detection and control capabilities in order to proactively avoid potential harm.

4.4. Contractor shall agree and warrant that while providing AI-based solutions under this agreement, they shall not engage in the creation, distribution, or dissemination of "Deepfakes". This includes, but is not limited to, the use of AI technologies for synthesizing or altering human images, videos, or voices in a manner that can mislead, deceive, or cause harm.

5. **Ongoing Monitoring and Maintenance.**

5.1. Contractor shall regularly monitor the performance of the AI solution to detect and rectify any unintended consequences or biases that may arise during its operation.

5.2. Contractor shall promptly address any identified issues to ensure the ongoing ethical and secure use of the AI solution.

5.3. Contractor shall immediately communicate the discovery of any unattended consequences or biases to Metro Government, including the potential impact to services.

6. **Liability and Accountability.**

6.1. Contractor shall assume responsibility for any negative consequences resulting from the AI solution's use, including breaches of data security, ethical violations, biases or intellectual property rights' violations.

6.2. Contractor shall indemnify Metro Government against any claims arising from Contractor's failure to comply with ethical, security, intellectual property laws or other legal standards in relation to the AI based solution.

7. **Compliance with Laws and Regulations.**

7.1. Contractor shall ensure that the AI solution complies with all applicable laws, regulations, and industry standards, such as the NIST AI Risk Management Framework.

7.2. Any changes in laws or regulations that impact the secure, ethical, and proper use of the AI solution shall be promptly addressed by Contractor and communicated to Metro Government with 24 hours of discovery.

7.3. Contractor shall ensure that all training data is legally obtained and its use is compliant under any applicable contractual, regulatory, or legal requirements and licensing agreements.

Agent Security and Training

1 **Background Check.** Contractor shall perform a background check which includes a criminal record check on all Agents, who may have access to Metro Government Information. Contractor shall not allow any Agents to access Metro Government Information or perform Services under a Purchasing Agreement if Contractor knows or reasonably should know that such Agent has been convicted of any felony or has been terminated from employment by any employer or contractor for theft, identity theft, misappropriation of property, or any other similar illegal acts.

2 **Information Security Officer.** If Agents will access or handle Metro Government Information, Contractor shall designate an Information Security Officer, who will be responsible for Contractor information security and compliance with the terms of this Agreement as it relates to Metro Government Information.

3 **Agent Access Control.** Contractor shall implement and maintain procedures to ensure that any Agent who accesses Metro Government Information has appropriate clearance, authorization, and supervision. These procedures must include:

  3.1 Documented authorization and approval for access to applications or information stores which contain Metro Government Information; e.g., email from a supervisor approving individual access (note: approver should not also have technical rights to grant access to Sensitive Information); documented role-based access model; and any equivalent process which retains documentation of access approval.

  3.2 Periodic (no less than annually) reviews of Agent user access rights in all applications or information stores which contain Sensitive Information. These reviews must ensure that access for all users is up-to-date, appropriate and approved.

  3.3 Termination procedures which ensure that Agent's user accounts are promptly deactivated from applications or information stores which contain Sensitive Information when users are terminated or transferred. These procedures must ensure that accounts are deactivated or deleted no more than 14 business days after voluntary termination, and 24 hours after for cause terminations.

  3.4 Procedures which ensure that Agent's user accounts in applications or information stores which contain Sensitive Information are disabled after a defined period of inactivity, no greater than every 180 days.

  3.5 Procedures which ensure that all Agents use unique authentication credentials which are associated with the Agent's identity (for tracking and auditing purposes) when accessing systems which contain Sensitive Information.

  3.6 Contractor will maintain record of all Agents who have been granted access to Metro Government Sensitive Information. Contractor agrees to maintain such records for the length of the agreement plus 3 years after end of agreement. Upon request, Contractor will supply Metro Government with the names and login IDs of all Agents who had or have access to Metro Government Information.

4 **Agent Training.**

  4.1 Contractor shall ensure that any Agent who access applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of the information or information and the security of the application. Completion of this training must be documented and must occur before Agent may access any Sensitive Information. This training must include, at a minimum:
    4.1.1   Appropriate identification and handling of Metro Government Information

4.1.1.1   Awareness of confidentiality requirements contained in this Agreement;

4.1.1.2   Procedures for encrypting Metro Government Information before emailing or transmitting over an Open Network, if the information classification of the information requires these controls;

4.1.1.3   Procedures for information storage on media or mobile devices (and encrypting when necessary).

4.1.2   Education about the procedures for recognizing and reporting potential Information Security Incidents;

4.1.3   Education about password maintenance and security (including instructions not to share passwords);

4.1.4   Education about identifying security events (e.g., phishing, social engineering, suspicious login attempts and failures);

4.1.5   Education about workstation and portable device protection; and

4.1.6   Awareness of sanctions for failing to comply with Contractor security policies and procedures regarding Sensitive Information.

4.1.7   Periodic reminders to Agents about the training topics set forth in this section.

4.2   Contractor shall ensure that any Agent who accesses applications or information stores which contain Metro Government Information are adequately trained on the appropriate use and protection of this information. Completion of this training must be documented and must occur before Agent may access any Metro Government Information. This training must include, at a minimum:

4.2.1   Instructions on how to identify Metro Government Information.

4.2.2   Instructions not to discuss or disclose any Sensitive Information to others, including friends or family.

4.2.3   Instructions not to take media or documents containing Sensitive Information home unless specifically authorized by Metro Government to do so.

4.2.4   Instructions not to publish, disclose, or send Metro Government Information using personal email, or to any Internet sites, or through Internet blogs such as Facebook or Twitter.

4.2.5   Instructions not to store Metro Government Information on any personal media such as cell phones, thumb drives, laptops, personal digital assistants (PDAs), unless specifically authorized by Metro Government to do so as part of the Agent's job.

4.2.6   Instructions on how to properly dispose of Metro Government Information, or media containing Metro Government Information, according to the terms in Exhibit DMH as well as applicable law or regulations.

5   Agent Sanctions. Contractor agrees to develop and enforce a documented sanctions policy for Agents who inappropriately and/or in violation of Contractor's policies and this Agreement, access, use or maintain applications or information stores which contain Sensitive Information. These sanctions must be applied consistently and commensurate to the severity of the violation, regardless of level within management, and including termination from employment or of contract with Contractor.

Protection Against Malicious Software

1   **Microsoft Systems on Metro Government Networks.** For Products which will be installed on Microsoft Windows Systems residing on Metro Government Network, Contractor warrants that the Product will operate in conjunction with Metropolitan Government Antivirus Software, and will use real time protection features.

2   **Non-Microsoft Systems on Metro Government Networks.** For Products installed on non-Microsoft Windows Systems residing on Metro Government Network, Contractor shall allow Metro Government to install Antivirus Software on such Products where technically possible. Upon Metro Government's request, Contractor shall provide the requisite information to implement such Antivirus Software in a manner which will not materially impact the functionality or speed of the Product.

Information Backup, Contingency Planning and Risk Management

1   General.

    1.1 Contractor agrees to backup Metro Government Information which Contractor maintains or Stores. Backup and restoration procedures and related infrastructure, including frequency of backup, offsite storage, media lifespan and media reliability, must be commensurate with the criticality and availability requirement of the Metro Government Information being backed up.

    1.2 Upon Metro Government's request, Contractor shall supply Metro Government with an inventory of Metro Government Information that Contractor Stores and/or backed up.

    1.3 Contractor shall periodically, no less often than annually, test backup tapes or media by restoring Metro Government Information to a system similar to the original system where the Metro Government Information are stored.

    1.4 Upon Metro Government's request, Contractor shall supply copies of Metro Government Information in a format requested by Metro Government.

    1.5 Contractor shall backup business critical information at a frequency determined by Metro Government business owner.

2   Storage of Backup Media. Contractor shall store archival and backup media in a secured offsite location. Upon request, Contractor will promptly notify Metro Government of the physical address of the offsite location. The backups of the information should be stored in a manner commensurate with the security around the information. The backup tapes should be encrypted if the sensitivity of the information requires that level of security.

3   Disaster Recovery Plan. Contractor will maintain a Disaster Recovery Plan for all applications or information stores which contain business critical information. This plan will outline the procedures necessary to restore business critical information on the application or systems in a timely fashion in the case of an emergency or disaster.

4   Emergency Mode Operation Plan. Contractor shall maintain an emergency mode operating plan which ensures that systems or applications using or accessing business critical information are operational during an emergency or natural disaster, or are made operational after a disaster in a prompt manner, commensurate with the criticality of the information on the system.

5   Testing and Revision Procedure. Contractor agrees to test, at least annually, Contractor Disaster Recovery Plan and emergency mode operations plan and maintain a documented procedure for such testing. Contractor shall document the results and findings from such testing and revise the plan accordingly.

6   Risk Management Requirements. Contractor shall implement internal risk management practices to ensure the confidentiality, integrity and availability of Metro Government Information. These practices will be no less secure than the ones used by Contractor to protect Contractor's own Sensitive Information or information of comparable sensitivity.

<div align="center">

SECTION CSP

Cloud Service and Hosted Service Providers

</div>

1 **Certifications and Compliance.**

    1.1. Contractor will, on at least an annual basis, hire a third party auditing firm to perform a Statement on Standards for Attestation Engagements (SSAE) No. 16 audit, or equivalent audit, on internal and external Contractor procedures and systems that access or contain Metro Data.

    1.2. Contractor shall adhere to SOC 1/SSAE 16 audit compliance criteria and data security procedures (or any successor report of a similar nature that is generally accepted in the industry and utilized by Contractor) applicable to Contractor.   Upon Metro's request, Contractor will provide Metro with a copy of the audit results set forth in Contractor's SOC 1/SSAE 16 audit report.

    1.3. Metro shall have the right to terminate this Agreement (together with any related agreements, including licenses and/or Statement(s) of Work) and receive a full refund for all monies prepaid thereunder in the event that the Contractor fails to produce an acceptable SSAE-16/ SOC-1 Type II report.

    1.4. The Contractor will ensure that its environment is compliant with the control standards of FISMA (Federal Information Security Management Act) 44 U.S.C. § 3541, et seq.), NIST standards in FIPS 140-2, FIPS 180, FIPS 198-1, FIPS 199, FIPS 200, FIPS 201 and NIST Special Publications 800-53, 800-59, and 800-60. In addition, the Contractor must provide Metro with any documentation it requires for its reporting requirements within 10 days of a request.

    1.5. Contractor agrees to comply with all applicable privacy laws.

2 **Data Security.**   Metro data, including but not limited to data hosted, stored, or held by the Contractor in the Product(s) or in the platform operated by Contractor, or on any device owned or in the custody of Contractor, its employees, agents or Contractors, will be encrypted. Contractor will not transmit any unencrypted Metro Data over the internet or a wireless network, and will not store any Metro Data on any mobile computing device, such as a laptop computer, USB drive or portable data device, except where there is a business necessity and then only if the mobile computing device is protected by industry-standard encryption software approved by Metro.

3 **Use of Subcontractors.** The Contractor shall retain operational configuration and control of data repository systems used to process and store Metro data to include any or remote work. In the event that the Contractor has subcontract the operational configuration and control of any Metro data, Contractor is responsible for ensuring that any third parties that provide services to the Contractor meets security requirements that the Contractor has agreed upon in this contract.

4 **Location of Data.** The Contractor shall maintain all data within the United States, which means the 50 States, the District of Columbia, and outlying areas. The Contractor shall provide Metro with a list of the physical locations that may contain Metro data within 20 days with updates on a quarterly basis.

5 **Personnel Access.** The Contactor will require all employees who will have access to Metro data, the architecture that supports Metro data, or any physical or logical devices/code to pass an appropriate background investigation.

6 **Asset Availability.**

    6.1. The Contractor must inform Metro of any interruption in the availability of the cloud service as required by the agreed upon service level agreement. Whenever there is an interruption in service, the Contractor must inform Metro of the estimated time that the system or data will be unavailable. The Contractor must provide regular updates to Metro on the status of returning the service to an operating state according to any agreed upon SLAs and system availability requirements.

    6.2. The Contractor shall be responsible for maintaining and ensuring continued compatibility and interoperability with Metro's systems, infrastructure, and processes for the term of the contract. In the event of an unavoidable compatibility and interoperability issue, the Contractor shall be responsible for providing timely notification to Metro and shall be responsible for working with Metro to identify appropriate remedies and if applicable, work with Metro to facilitate a smooth and seamless transition to an alternative solution and/or provider.

7 **Misuse of Metro Data and Metadata.**

    7.1. The Contractor shall not access, use, or disclose Metro data unless specifically authorized by the terms of this contract or a task order issued hereunder. If authorized by the terms of this contract or a task order issued hereunder, any access to, or use or disclosure of, Metro data shall only be for purposes specified in this contract or task order. Contractor shall ensure

that each of its employees and representatives, and any others (e.g., subcontractor employees) performing duties hereunder, shall, prior to obtaining access to any Metro data, sign a contract or task order specific nondisclosure agreement.

7.2. The Contractor shall use Metro-related data only to manage the operational environment that supports Metro data and for no other purpose unless otherwise permitted with the prior written approval of the Contracting Officer. A breach of the obligations or restrictions may subject the Contractor to criminal, civil, administrative, and contractual actions in law and equity for penalties, damages, and any other appropriate remedies by any party adversely affected by the breach.

8   Data Breach and Incident Reporting.

8.1. The Contractor will submit reports of cyber incidents through approved reporting mechanisms. The Contractor's existing notification mechanisms that are already in place to communicate between the Contractor and its customers may be used, as long as those mechanisms demonstrate a level of assurance, equivalent to the listed encrypted mechanisms, for the confidentiality and integrity of the information.

8.2. The Contractor will use a template format when reporting initial incidents by secure fax, telephonically, or by other electronic means. Initial reports may be incomplete. Reporting should balance the necessity of timely reporting (reports with critical information) versus complete reports (those with all blocks completed). Timely reporting is vital, and complete information should follow as details emerge.

8.3. In addition to the above, if the incident concerns a breach of PII or a potential breach of PII, the Contractor will report to the contracting officer's designee within 24 hours of the discovery of any data breach. The Contractor shall provide Metro with all information and cooperation necessary to enable compliance by the Contractor and/or Metro with data breach reporting and mitigation actions required by applicable law, regulation, policy, and this contract.

9   Facility Inspections. The Contractor agrees to have an independent third party or other industry recognized firm, which has been approved by Metro, conduct a security audit based on Metro's criteria as needed, but no more than once a year. The audit results and Contractor's plan for addressing or resolving of the audit results shall be shared with Metro within 20 days of the Contractor's receipt of the audit results.

10   Law Enforcement.

10.1. The Contractor shall record all physical access to the cloud storage facilities and all logical access to Metro data. This may include the entrant's name, role, purpose, account identification, entry and exit time.

10.2. If Metro data is co-located with the non-Metro data, the Contractor shall isolate Metro data into an environment where it may be reviewed, scanned, or forensically evaluated in a secure space with access limited to authorized Metro personnel identified by the Metro personnel, and without the Contractor's involvement.

11   Maintenance. The Contractor shall be responsible for all patching and vulnerability management (PVM) of software and other systems' components supporting services provided under this agreement to prevent proactively the exploitation of IT vulnerabilities that may exist within the Contractor's operating environment. Such patching and vulnerability management shall meet the requirements and recommendations of NIST SP 800-40, with special emphasis on assuring that the vendor's PVM systems and programs apply standardized configurations with automated continuous monitoring of the same to assess and mitigate risks associated with known and unknown IT vulnerabilities in the Contractor's operating environment. Furthermore, the Contractor shall apply standardized and automated acceptable versioning control systems that use a centralized model to capture, store, and authorize all software development control functions on a shared device that is accessible to all developers authorized to revise software supporting the services provided under this agreement. Such versioning control systems shall be configured and maintained to assure all software products deployed in the Contractor's operating environment and serving Metro are compatible with existing systems and architecture of Metro.

12   Notification. The Contractor shall notify Metro within 60 minutes of any warrants, seizures, or subpoenas it receives that could result in the loss or unauthorized disclosure of any Metro data. The Contractor shall cooperate with Metro to take all measures to protect Metro data from any loss or unauthorized disclosure that might reasonably result from the execution of any such warrant, seizure, subpoena, or similar legal process.

13   Supply Chain. The Contractor is responsible for exercising due diligence to use genuine hardware and software products that are free of malware.

14   Service Level Agreements. The Contractor shall work with Metro to develop a service level agreement, including defining roles, responsibilities, terms, and clear measures for performance by Contractor.

Development

1   **Source Code License/Source Code Escrow.** Source code is to be provided to either Metro Government or an escrow agent as a deliverable of any software development project or any other projects which requires code to be created as a deliverable and after any updates to code. Contractor must provide proof that all source code provided to Metro Government or to escrow agent is complete, up to date and includes all components necessary to function in production environment.   Said source code shall be considered the Confidential Information of Contractor or its successor and Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement.

  1.1   **Source Code License.** Contractor agrees to provide Metro Government a source code license and will provide, as part of deliverable, source code that is developed as part of this contract, including any customizations. Source code to be provided in an agreed upon media and will be provided within 30 days after any updates. Any third party libraries used in the development of the software will also be included. Documentation provided must be sufficient for a developer versed in the applicable programming language to fully understand source code.

  1.2   **Source Code Escrow.** In the event that (i) Contractor becomes insolvent or bankrupt, (ii) Contractor makes an assignment for the benefit of creditors, (iii) Contractor consents to a trustee or receiver appointment, (iv) a trustee or receiver is appointed for Contractor or for a substantial part of its property without its consent, (v) Contractor voluntarily initiates bankruptcy, insolvency, or reorganization proceedings, or is the subject of involuntary bankruptcy, insolvency, or reorganization proceedings, or (vi) Contractor announces that it has entered into an agreement to be acquired by a then named Competitor, then Contractor will negotiate in good faith to enter into a source code escrow agreement with a mutually agreed source code escrow company setting forth source code escrow deposit procedures and source code release procedures relating to the software provided as part of this contract. Notwithstanding the foregoing, the escrow instructions shall provide for a release of the source code to Metro Government only upon the occurrence of (a) the filing of a Chapter 7 bankruptcy petition by Contractor, or a petition by Contractor to convert a Chapter 11 filing to a Chapter 7 filing; (b) the cessation of business operations by Contractor; or (c) the failure on the part of Contractor to comply with its contractual obligations to Metro Government to comply with its maintenance and support obligations for a period of more than thirty (30) days after it has received written notice of said breach. In the event of a release of source code pursuant to this section, said source code shall continue to be the Confidential Information of Contractor or its successor in interest In the event of a release of source code to Metro Government from escrow, Metro Government may only use, copy and/or modify the source code consistent with the purposes of this agreement (or have a contractor who has agreed in writing to confidentiality provisions as restrictive as those set forth in this Agreement do so on its behalf).

2   **Mobile Applications Security.** Contractor shall have the ability/expertise to develop secure mobile applications. Specifically, an awareness of secure mobile application development standards, such as OWASP's Mobile Security project. Development should be able to meet at a minimum OWASP's MASVS-L1 security standard or a similar set of baseline security standards as agreed upon by Metro Government.

Device and Storage Media Handling

1   **Portable Media Controls.** Contractor (including its Agents) shall only store Metro Government Information on portable device or media when expressly authorized by Metro Government to do so. When Contractor stores Metro Government Sensitive Information or on portable device or media, Contractor shall employ the following safeguards:

 1.1 Access to the device or media shall require a password or authentication;

 1.2 The device or media shall be encrypted using Strong Encryption;

 1.3 The workstation or portable device or media containing Metro Government Information must be clearly identified or labeled in such a way that it can be distinguished from other media or device which is not used to store Sensitive Information.

 1.4 The device or media must be accounted for by a system or process which tracks the movements of all devices or media which contain Metro Government Information**.**

2   **Media Disposal.**

 2.1 Contractor shall only dispose of media containing Metro Government Information when authorized by Metro Government.

 2.2 Contractor shall dispose of any media which stores Metro Government Information in accordance with media sanitization guidelines for media destruction as described in NIST document NIST SP800-88: Guidelines for Media Sanitization.

 2.3 Upon Metro Government request, Contractor shall promptly provide written certification that media has been properly destroyed in accordance with this Agreement.

 2.4 Contractor may not transport or ship media containing Metro Government Information unless the media is Encrypted using Strong Encryption, or the information on the media has been sanitized through complete information overwrite (at least three passes); or media destruction through shredding, pulverizing, or drilling holes (e.g. breaking the hard drive platters).

3   **Media Re-Use.**

 3.1 Contractor shall not donate, sell, or reallocate any media which stores Metro Government Information to any third party, unless explicitly authorized by Metro Government**.**

 3.2 Contractor shall sanitize media which stores Metro Government Information before reuse by Contractor within the Contractor facility.

SECTION ENC

Encryption and Transmission of Information

1   Contractor shall Encrypt Metro Government Sensitive Information whenever transmitted over the Internet or any untrusted network using Strong Encryption. Encryption of Sensitive Information within the Metro Government Network, or within Contractor's physically secured, private information center network, is optional but recommended.

2   Contractor shall Encrypt Metro Government Authentication Credentials while at rest or during transmission using Strong Encryption.

3   Contractor shall Encrypt, using Strong Encryption, all Sensitive Information that is stored in a location which is accessible from Open Networks.

4   If information files are to be exchanged with Contractor, Contractor shall support exchanging files in at least one of the Strongly Encrypted file formats, e.g., Encrypted ZIP File or PGP/GPG Encrypted File.

5   All other forms of Encryption and secure hashing must be approved by Metro Government.

Incident Response

1 **Incident Reporting.** Contractor shall report any Information Security Incident of which it becomes aware, or failure of any technical or procedural controls, which has or had a potential to affect Metro Government Network, Metro Government Infrastructure or Metro Government Information to Metro Government and according to the following timeline and procedure:

  1.1 Contractor shall promptly report to Metro Government any successful Information Security Incident (with or without actual harm to system or information) within 24 hours of becoming aware of the incident. At a minimum, such report shall contain: (a) date and time when the Information Security Incident occurred; (b) the date and time when such incident was discovered by Contractor; (b) identification of the systems, programs, networks and/or Metro Government Information affected by such incident; (c) preliminary impact analysis; (d) description and the scope of the incident; and (e) any mitigation steps taken by Contractor However, if Contractor is experiencing or has experienced a Information Breach or a successful Information Security Incident to systems that host or Store Sensitive Information or an Information Security Incident that is causing or has caused material disruption to the functionality or operation of Contractor systems or damage to Contractor hardware, software or information, including a successful attack by Malicious Software, Contractor shall report such security breach or incident to Metro Government both to the ITS Help Desk at (615) 862-HELP and to the Metro Government department within 24 hours from Contractor's reasonable awareness of such security breach or incident.

  1.2 Contractor shall document any attempted but unsuccessful Information Security Incident of which it becomes aware and report to Metro Government upon its request. The frequency, content, and format of such report will be mutually agreed upon by the parties.

2 **Incident Response.**

  2.1 Contractor shall have a documented procedure for promptly responding to an Information Security Incidents and Information Breach that complies with applicable law and shall follow such procedure in case of an incident. Contractor shall have clear roles defined and communicated within its organization for effective internal incidence response.

  2.2 Contractor shall designate a contact person for Metro Government to contact in the event of an Information Security Incident. This contact person should possess the requisite authority and knowledge to: (i) act as a liaison to communicate between Contractor and Metro Government regarding the incident (including providing information requested by Metro Government); (ii) perform the reporting obligations of Contractor under this exhibit; and (iii) develop a mitigation strategy to remedy or mitigate any damage to Metro Government Network, Metro Government Infrastructure, Metro Government Information or the Product or Service provided to Metro Government that may result from the Information Security Incident.

Audit Logs

1 **Audit Log Information**. The Product or Service will provide user activity Audit Log information. Audit Log entries must be generated for the following general classifications of events: login/logout (success and failure); failed attempts to access system resources (files, directories, information bases, services, etc.); system configuration changes; security profile changes (permission changes, security group membership); changes to user privileges; actions that require administrative authority (running privileged commands, running commands as another user, starting or stopping services, etc.); and remote control sessions (session established, login, logout, end session, etc.). Each Audit Log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (system name, port, etc.).

2 **Audit Log Integrity.** Contractor shall implement and maintain controls to protect the confidentiality, availability and integrity of Audit Logs.

3 **User Access Audit.** Upon Metro Government's request, Contractor shall provide Audit Logs of Metro Government's users of the Product or Service to Metro Government.

4 **Audit Log Feed.** Upon request, Contractor shall implement a regular, but in no event less than daily, automated Audit Log feed via a secured, persistent connection to Metro Government Network so that Metro Government may monitor or archive Audit Log information relating to Metro Government's users on Metro Government systems.

5 **Audit Log Availability.**

   5.1 Contractor shall ensure that Audit Logs for the Product or Service for the past 90 days are readily accessible online.

   5.2 If for technical reasons or due to an Information Security Incident, the online Audit Logs are not accessible by Metro Government or no longer trustworthy for any reason, Contractor shall provide to Metro Government trusted Audit Log information for the past 90 days within 2 business days from Metro Government's request.

   5.3 Contractor shall provide or otherwise make available to Metro Government Audit Log information which are 91 days or older within 14 days from Metro Government's request.

   5.4 Contractor shall make all archived Audit Logs available to Metro Government no later than thirty (30) days from Metro Government's request and retrievable by Metro Government for at least one (1) year from such request.

   5.5 Contractor shall agree to make all Audit Logs available in an agreed upon format.

Network Security

1   **Network Equipment Installation.**

    1.1 Contractor shall not install new networking equipment on Metro Government Network without prior written permission by the Metro Government ITS department. Contractor shall not make functional changes to existing network equipment without prior written consent of such from Metro Government ITS department.

    1.2 Contractor shall provide the Metro Government ITS department contact with documentation and a diagram of any new networking equipment installations or existing networking equipment changes within 14 days of the new installation or change.

    1.3 Contractor shall not implement a wireless network on any Metro Government site without the prior written approval of the Metro Government ITS contact , even if the wireless network does not connect to the Metro Government Network. Metro Government may limit or dictate standards for all wireless networking used within Metro Government facility or site.

2   **Network Bridging.** Contractor shall ensure that no system implemented or managed by Contractor on the Metro Government Network will bridge or route network traffic.

3   **Change Management.** Contractor shall maintain records of Contractor installations of, or changes to, any system on the Metro Government Network. The record should include date and time of change or installation (start and end), who made the change, nature of change and any impact that the change had or may have to the Metro Government Network, Metro Government system or Metro Government Information.

4   **System / Information Access.**

    4.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

    4.2 Contractor shall only use Metro Government approved methods to configure Metro Government systems or application or grant access to systems.

    4.3 Contractor shall use the Principle of Least Privilege when granting access to Metro Government Information, network or systems.

SECTION PAT

Patch Creation and Certification

1 **Security Patch Required.** Unless otherwise expressly agreed by Metro Government and Contractor, for Products that are no longer under performance warranty, Contractor shall provide no less than standard maintenance and support service for the Products, which service includes providing Security Patches for the Products, for as long as Metro Government is using the Products.

2 **Timeframe for Release.** For Vulnerabilities contained within the Product that are discovered by Contractor itself or through Responsible Disclosure, Contractor shall promptly create and release a Security Patch. Contractor must release a Security Patch: (i) within 90 days for Critical Vulnerabilities, (ii) within 180 days for Important Vulnerabilities, and (iii) within one (1) year for all other Vulnerabilities after Contractor becomes aware of the Vulnerabilities. For Vulnerabilities contained within the Product that have become publicly known to exist and are exploitable, Contractor will release a Security Patch in a faster timeframe based on the risk created by the Vulnerability, which timeframe should be no longer than thirty (30) days. For the avoidance of doubt, Contractor is not responsible for creation of Security Patches for Vulnerabilities in the Product that is caused solely by the Off-the-Shelf Software installed by Metro Government.

3 **Timeframe for Compatibility Certification.** Contractor shall promptly Certify General Compatibility of a Security Patch for third party software which the Product is dependent upon when such patch is released. For a Security Patch for Microsoft Windows Operating Systems, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days, and shall Certify General Compatibility of an Important Security Patch within thirty (30) days, from the release of the patch. For Security Patches for Off-the-Shelf Software (OTS), Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and Certify General Compatibility of an Important Security Patch within thirty (30) days from its release. For Security Patch for all other third party software or system, Contractor shall Certify General Compatibility of a Critical Security Patch within five (5) days and an Important Security Patch within thirty (30) days from its release. . Contractor shall publish whether the Security Patches are generally compatible with each related Product.

4 **Notice of Un-patchable Vulnerability.**   If Contractor cannot create a Security Patch for a Vulnerability, or Certify General Compatibility of a Security Patch for OTS software, within the timeframe specified herein, Contractor shall notify Metro Government of the un-patchable Vulnerability in writing. Such notice shall include sufficient technical information for Metro Government to evaluate the need for and the extent of immediate action to be taken to minimize the potential effect of the Vulnerability until a Security Patch or any other proposed fix or mitigation is received.

5 **Vulnerability Report.** Contractor shall maintain a Vulnerability Report for all Products and Services and shall make such report available to Metro Government upon request, provided that Metro Government shall use no less than reasonable care to protect such report from unauthorized disclosure. The Vulnerability Report should (a) identify and track all known Vulnerabilities in the Products or Services on a continuing and regular basis, (b) document all Vulnerabilities that are addressed in any change made to the Product or Service, including without limitation Security Patches, upgrades, service packs, updates, new versions, and new releases of the Product or Service, (c) reference the specific Vulnerability and the corresponding change made to the Product or Service to remedy the risk, (d) specify the critical level of the Vulnerability and the applicable Security Patch, and (e) other technical information sufficient for Metro Government to evaluate the need for and the extent of its own precautionary or protective action. Contractor shall not hide or provide un-documented Security Patches in any type of change to their Product or Service.

6 **SCCM Compatibility for Windows Based Products.** Contractor Patches for Products that operate on the Microsoft Windows Operating System must be deployable with Microsoft's System Center Configuration Manager.

SECTION PES

Physical and Environmental Security

Contractor shall implement security measures at any Contractor facilities where Sensitive Information is stored. Such security measures must include, at a minimum:

1 **Contingency Operations.** A documented Disaster Recovery Plan for accessing the facility and the Sensitive Information, and restoring Sensitive Information if needed, in the case of an emergency or crisis.

2 **Environmental Safeguards**. Reasonable environmental safeguards to protect systems storing Sensitive Information from smoke, heat, water, fire, humidity, or power surge damage.

3 **Access Control.** Appropriate controls which ensure that only authorized personnel are allowed physical access to the facility. Examples of appropriate controls include, but are not limited to: signage; personnel badges and controlled badge access; visitor sign in, escort, and sign out; security guards; and video surveillance for information centers which store Sensitive Information.

4 **Maintenance Records.** Contractor shall conduct regular maintenance on systems which contain Sensitive Information and to facility's physical and environmental controls (e.g., temperature, physical access). Contractor shall maintain documentation of any repairs or maintenance performed on the systems or facility and shall provide Metro Government a copy of such records upon its reasonable request.

5 **Physical Safeguards.** Contractor shall use best efforts to prevent theft or damage to Contractor systems or storage media containing Sensitive Information. Such efforts shall include, but are not limited to:

   5.1 Protecting systems or devices that contain un-encrypted Sensitive Information with physical barriers such as locked cabinet, floor to ceiling room, or secured cage.

   5.2 Not storing Un-encrypted Sensitive Information in "multi-party" shared physical environments with other entities.

   5.3 Not transporting or shipping un-encrypted media which stores Sensitive Information unless the information is sanitized through full media overwrite (at least one complete pass), or media destruction through shredding, pulverizing, or drive-punching (e.g., breaking the hard drive platters).

   5.4 In the event Products generate, store, transmit or process Sensitive Information and the Product does not support encryption, Contractor shall be solely responsible for the provision of physical security measures for the applicable Products (e.g., cable locks on laptops).

<div align="center">**SECTION REM**</div>

<div align="center">**Remote Access to Metro Government Network/System**</div>

1   B2B VPN or Private Circuit Requirements.

    1.1 For Contractor's Business to Business ("B2B") or private circuit network connections which terminate on the outside of the Metro Government Network, Contractor must protect such connections by an International Computer Security Association Labs certified firewall.

    1.2 Government may deny any traffic type due to risk and require Contractor to use a more secured protocol. Microsoft protocols such as those used in Window File Shares are considered risky and will not be allowed.

    1.3 B2B Virtual Private Network ("VPN") connections to the Metro Government Network will only terminate on Metro Government managed network infrastructure.

    1.4 Contractor shall authenticate the VPN to the Metro Government Network using at least a sixteen (16) character pre-shared key that is unique to the Metro Government.

    1.5 Contractor shall secure the VPN connection using Strong Encryption.

    1.6 Contractor shall connect to the Metro Government Network using a device capable of Site-to-Site IPSec support.

    1.7 Contractor shall connect to the Metro Government Network using a device capable of performing policy-based Network Address Translation (NAT).

    1.8 Contractor shall connect to the Metro Government Network through the Metro Government VPN concentrator.

    1.9 Contractor shall not implement any form of private circuit access to the Metro Government network without prior written approval from the Metro Government ITS Department.

    1.10 Metro Government reserves the right to install filtering or firewall devices between Contractor system and the Metro Government Network.

2   Requirements for Dial-In Modems.

    2.1 If Contractor is using an analog line, the analog line shall remain disconnected from the modem when not in use, unless Metro Government has expressly authorized permanent connection.

    2.2 Contractor shall provide the name of the individual(s) connecting to Metro Government Network and the purpose of the connection when requesting connectivity.

3   System / Information Access. Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

4   Remote Access Account Usage.

    4.1 Upon request, Contractor shall provide Metro Government with a list of active Agent user accounts and access levels and other information sufficient for Metro Government to deactivate or disable system access if it deems appropriate.

    4.2 Contractor may not share Metro Government-issued ID's, or any user accounts which grant access to Metro Government Network or Metro Government systems.

4.3 Contractor Agent shall use unique accounts assigned to the Agent to perform work. Service accounts (or accounts that are configured and used by systems to gain access to information or other systems) may not be used by Contractor Agents to access any system.

5   **Metro Government Network Access Requirements.**

5.1 Contractor shall only use Contractor systems which are compatible with Metro Government Remote Access technology to access Metro Government Network. If Contractor does not have a system that is compatible, it is Contractor's responsibility to obtain a compatible system.

5.2 Contractor shall implement security controls to protect Metro Government Network from risk when its systems or Agents connect to the Metro Government Network. Such controls include, but are not limited to:

     5.2.1 Installing and maintaining ICSA Labs certified Anti-virus Software on Contractor system and, to the extent possible, use real time protection features. Contractor shall maintain the Anti-virus Software in accordance with the Anti-virus Software Contractor's recommended practices.

     5.2.2 Contractor may not access the Metro Government Network with systems that may allow bridging of the Metro Government Network to a non-Metro Government network.

     5.2.3 Contractor shall only access the Metro Government Network with systems that have the most current Security Patches installed.

6   **Use of Remote Support Tools on Metro Government Network.**

6.1 Contractor shall connect to the Metro Government Network using only Metro Government provided or approved Remote Access Software.

6.2 Contractor shall not install or implement any form of permanent Remote Access (e.g., GotoMyPC) on the Metro Government Network or Metro Government systems.

7   **Remote Control Software**

7.1 Contractor may not install any form of Remote Control Software on systems that are maintained or administered by Metro Government without Metro Government's consent. Contractor is only allowed to install Remote Control Software on Contractor Managed Systems.

7.2 Remote Control Software must secure all network traffic using Strong Encryption.

7.3 Contractor shall ensure that Remote Control Software contained within the Product supports the logging of session establishment, termination, and failed login attempts. Each log entry must include the following information about the logged event: date and time of event; type of event; event description; user associated with event; and network identifiers (IP address, MAC Address, etc.) or logical identifiers (System name, port, etc.). For Contractor Maintained Systems, Contractor shall ensure that such systems are configured to do the above.

7.4 Remote Control Software shall not provide escalation of user account privileges.

7.5 Contractor shall only access the Metro Government Network via Metro Government approved remote access methods. Contractor shall not supply Products, nor make configuration changes that introduce non-approved forms of Remote Access into the Metro Government Network.

<div align="center">**SECTION SOFT**</div>

<div align="center">**Software / System Capability**</div>

1   Supported Product.

   1.1 Unless otherwise expressly agreed by Metro Government in writing, Contractor shall provide Metro Government only supported versions of the Product, which will not become "end of life" for at least 24 months. When the Product or Service requires third party components, Contractor must provide a Product that is compatible with currently supported third party components. Unless otherwise expressly agreed by Metro Government, Contractor represents that all third party components in its Product are currently supported, are not considered "end of life" by the third party provider of such components, and will not become "end of life" in less than 24 months from the date of acquisition by Metro Government.

   1.2 If Open Source Software is incorporated into the Product, Contractor shall only use widely supported and active Open Source Software in the Product, and shall disclose such software to Metro Government prior to its acquisition of the Product.

   1.3 Information transfers within applications and involving services should be done using web services, APIs, etc. as opposed to flat file information transport.

2   Software Capabilities Requirements.

   2.1 Contractor shall disclose to Metro Government all default accounts included in their Product or provide a means for Metro Government to determine all accounts included in the Product.

   2.2 Contractor shall not include fixed account passwords in the Product that cannot be changed by Metro Government. Contractor shall allow for any account to be renamed or disabled by Metro Government.

   2.3 Contractor's Product shall support a configurable Session Timeout for all users or administrative access to the Product.

   2.4 Contractor shall ensure that the Product shall transmit and store Authentication Credentials using Strong Encryption.

   2.5 Contractor Products shall mask or hide the password entered during Interactive User Login.

   2.6 Contractor shall ensure that Products provided can be configured to require a Strong Password for user authentication.

   2.7 Contractor's Product shall allow user accounts to be disabled after a configurable amount of failed login attempts over a configurable amount of time.

   2.8 Contractor's Product shall have the capability to require users to change an initial or temporary password on first login.

   2.9 Contractor's Product shall have the capability to report to Metro Government, on request, all user accounts and their respective access rights within three (3) business days or less of the request.

   2.10 Contractor's Product shall have the capability to function within Metro Governments Information Technology Environment. Specifications of this environment are available upon request.

3   Backdoor Software. Contractor shall not provide Products with Backdoor Software, including, without limitation, undocumented or secret access functions (e.g., accounts, authorization levels, over-rides or any backdoor). Contractor shall supply all information needed for the Metro Government to manage all access (local or remote) capabilities within the Product including denying of Remote Access entirely from any party including Contractor. Contractor shall not include any feature within the Product that would allow anyone to circumvent configured authorization remotely.

<u>**SECTION VMGT**</u>

Contractor Managed System Requirements

1   <u>**Vulnerability and Patch Management.**</u>

   1.1 For all Contractor Managed Systems that store Metro Government Information, Contractor will promptly address Vulnerabilities though Security Patches. Unless otherwise requested by Metro Government, Security Patches shall be applied within fourteen (14) days from its release for Critical Security Patches, thirty (30) days for Important Security Patches, and twelve (12) months for all other applicable Security Patches. Contractor may provide an effective technical mitigation in place of a Security Patch (if no Security Patch is available or if the Security Patch is incompatible) which doesn't materially impact Metro Government's use of the system nor require additional third party products.

   1.2 If the application of Security Patches or other technical mitigations could impact the operation of Contractor Managed System, Contractor agrees to install patches only during Metro Government approved scheduled maintenance hours, or another time period agreed by Metro Government.

   1.3 Contractor Managed Systems on the Metro Government Network or Metro Government Infrastructure, the Metro Government retains the right to delay patching for whatever reason it deems necessary.

   1.4 Metro Government will monitor compliance and check for Vulnerabilities on all Products on the Metro Government Network or Metro Government Infrastructure. Contractor shall provide Metro Government administrative credentials upon request for the purpose of monitoring compliance of a given Product. Metro Government will not knowingly change configurations of the Contractor Managed Systems without prior approval from Contractor.

   1.5 Government may monitor compliance of Contractor Managed Systems. Contractor agrees to allow Metro Government to check for Vulnerabilities during agreed upon times using mutually agreed upon audit methods.

   1.6 Contractor shall use all reasonable methods to mitigate or remedy a known Vulnerability in the Contractor Managed System according to the level of criticality and shall cooperate fully with Metro Government in its effort to mitigate or remedy the same. Upon Metro Government's request, Contractor shall implement any reasonable measure recommended by Metro Government in connection with Contractor's mitigation effort.

2   <u>**System Hardening.**</u>

   2.1 Contractor Managed Systems, Contractor shall ensure that either: (i) file shares are configured with access rights which prevent unauthorized access or (ii) Contractor shall remove or disable file shares that cannot be configured with access controls set forth in (i) hereof. Access rights to file shares that remain under (i) must use the Principle of Least Privilege for granting access.

   2.2 In the event that Contractor is providing Products or systems that are to be directly accessible from the Internet, Contractor shall disable or allow disabling by Metro Government of all active or executed software components of the Product or system that are not required for proper functionality of the Product or system.

   2.3 Contractor shall ensure that Contractor Managed Systems are synchronized with reliable time sources and have the proper time zone set or no time offset (e.g., GMT or UTC). In the case of systems residing on the Metro Government Network, Contractor shall ensure that all such systems are synchronized with an Metro Government corporate timeserver in their respective Regional Information Centers (RDC).

   2.4 For Contractor Managed Systems, Contractor shall remove or disable any default or guest user accounts. Default accounts that cannot be removed or disabled must have their default password changed to a Strong Password that is unique to the respective site and Metro Government.

   2.5 For Contractor Managed Systems, Contractor shall ensure that the system is configured to disable user accounts after a certain number of failed login attempts have occurred in a period of time less than thirty (30) minutes of the last login attempt or that system monitoring and notification is configured to alert system administrators to successive failed login attempts for the same user account.

3 **Authentication**.

    3.1 Contractor shall assign a unique user ID to any Agent or end user who accesses Sensitive Information on Contractor Managed Systems. This unique ID shall be configured so that it enables tracking of each user's activity within the system.

    3.2 Contractor agrees to require authentication for access to Sensitive Information on Contractor Managed System.

    3.3 Contractor agrees to configure the system to support Strong Authentication for accessing Sensitive Information from any Open Network (e.g., Internet, open wireless).   For avoidance of doubt, Metro Government Network is considered a trusted network.

    3.4 Contractor shall configure the system to expire passwords at least every one-hundred and eighty (180) days and require a password change on the next successful login. For system that cannot support Strong Passwords, Contractor shall configure the system to expire passwords every ninety (90) days.

    3.5 Unless otherwise agreed by Metro Government, Contractor shall ensure that Contractor Managed Systems will require Strong Password for user authentication.

4 **Automatic Log off.** Contractor shall configure systems which store Sensitive Information to automatically logoff user sessions at the most after 20 minutes of inactivity.

5 **User Accountability.** Contractor shall report to Metro Government, on request, all user accounts and their respective access rights within the system within five (5) business days or less of the request.

6 **Information Segregation, Information Protection and Authorization.** Contractor shall implement processes and/or controls to prevent the accidental disclosure of Metro Government Sensitive Information to other Contractor Metro Governments, including an Affiliates of Metro Government.

7 **Account Termination**. Contractor shall disable user accounts of Agents or Metro Government end users for the system within five (5) business days of becoming aware of the termination of such individual. In the cases of cause for termination, Contractor will disable such user accounts as soon as administratively possible.

8 **System / Information Access.**

    8.1 Contractor and its Agents shall only access system, application or information which they are expressly authorized by Metro Government to access, even if the technical controls in the system or application do not prevent Contractor or its Agent from accessing those information or functions outside of Metro Government's authorization. Contractor shall impose reasonable sanctions against any Agent who attempts to bypass Metro Government security controls.

    8.2 Contractor agrees to use the Principle of Least Privilege when granting access to Contractor Managed Systems or Metro Government Information.

9 **System Maintenance.**

    9.1 Contractor shall maintain system(s) that generate, store, transmit or process Metro Government Sensitive Information according to manufacturer recommendations. Contractor shall ensure that only those personnel certified to repair such systems are allowed to provide maintenance services.

    9.2 Contractor shall keep records of all preventative and corrective maintenance on systems that generate, store, transmit or process Metro Government Sensitive Information. Such records shall include the specific maintenance performed, date of maintenance, systems that the maintenance was performed on including identifiers (e.g., DNS name, IP address) and results of the maintenance. Upon request by Metro Government, Contractor shall supply such record within thirty (30) days.

<u>**SECTION BAA**</u>

HIPAA Business Associate Agreement

This Agreement is initiated by and between **THE METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY (METRO)**, a metropolitan form government organized and existing under the laws and constitution of the State of Tennessee ("**Metro**" or "**Covered entity**") and the Contractor("**Business Associate**").

SECTION 1 - DEFINITIONS

a. **Business Associate**. "Business Associate" shall generally have the same meaning as the term "Business Associate" in 45 CFR § 160.103, and in reference to the party to this agreement, shall mean the Contractor.

b. **Covered Entity.** "Covered Entity" shall generally have the same meaning as the term "covered entity" at 45 CFR § 160.103, and in reference to the party to this agreement, shall mean <u>**Metro**</u>. which must fall under one of the following categories:

    (1) A health plan.

    (2) A health care clearinghouse.

    (3) A health care provider who transmits any health information in electronic form in connection with a transaction covered by this subchapter.

c. **Disclosure.** "Disclosure" means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

d. **Electronic Media.** "Electronic Media" shall have the same meaning as set forth in 45 CFR § 160.103.

e. **Employer. "Employer" is defined as it is in 26 U.S.C. § 3401(d).**

f. **Genetic Information.** "Genetic Information" shall have the same meaning as set forth in 45 CFR § 160.103.

g. **HITECH Standards**. "HITECH Standards" means the privacy, security and security Breach notification provisions under the Health Information Technology for Economic and Clinical Health (HITECH) Act, Final Rule of 2013, and any regulations promulgated thereunder.

h. **Individual.** "Individual" shall have the same meaning as set forth in 45 CFR § 160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR § 164.502(g).

i. **Person.** "Person" means a natural person, trust or estate, partnership, corporation, professional association or corporation, or other entity, public or private.

j. **Privacy Rule.** "Privacy Rule" shall mean the Standards for Privacy of Individually Identifiable Health Information at 45 CFR Part 160 and Part 164, Subparts A and E.

k. **Protected Health Information.** "Protected Health Information" or "PHI":

    (1)   Shall have the same meaning as set forth in 45 CFR § 160.103.

    (2)   Includes, as set forth in 45 CFR § 160.103, any information, *now also including genetic information*, whether oral or recorded in any form or medium, that:

        (i)   Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

        (ii)   Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

l. **Required By Law.** "Required By Law" shall have the same meaning as the term "required by law" in 45 CFR § 164.103.

m. **Secretary.** "Secretary" shall mean the Secretary of the Department of Health and Human Services or his designee.

n. **Security Rule**. "Security Rule" shall mean the Standards for Security of Individually Identifiable Health Information at 45 CFR part 160 and subparts A and C of part 164.

o. **Subcontractor.** "Subcontractor" means a person to whom a business associate delegates a function, activity, or service, other than in the capacity of a member of the workforce of such business associate.

p. **Transaction.** "Transaction" shall have the same meaning as set forth in 45 CFR § 160.103.

q. **Catch-all definition.** Terms used but not otherwise defined in this Agreement shall have the same meaning as the meaning ascribed to those terms in the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"), the Health Information Technology Act of 2009, as incorporated in the American Recovery and Reinvestment Act of 2009 ("HITECH Act"), implementing regulations at 45 Code of Federal Regulations Parts 160-164 and any other current and future regulations promulgated under HIPAA or the HITECH Act.

SECTION 2 - OBLIGATIONS AND ACTIVITIES OF BUSINESS ASSOCIATE

a.   **Permitted Uses of Protected Health Information**. Business Associate shall not use or disclose Protected Health Information other than as permitted or required by this Agreement or as Required by Law. Business Associate may: 1) use and disclose PHI to perform its obligations under its contract with Metro; (2) use PHI for the proper management and administration of Business Associate; and (3) disclose PHI for the proper management and administration of Business Associate, if such disclosure is required by law or if Business Associate obtains reasonable assurances from the recipient that the recipient will keep the PHI confidential, use or further disclose the PHI only as required by law or such disclosure is authorized by Metro.

b.   **Safeguards.** Business Associate shall use appropriate administrative, physical and technical safeguards to prevent use or disclosure of the Protected Health Information other than as provided for by this Agreement. Business Associate shall develop and implement policies and procedures that comply with the Privacy Rule, Security Rule, and the HITECH Act. The Business Associate must obtain satisfactory assurances that any subcontractor(s) will appropriately safeguard PHI.

c.   **Mitigation.** Business Associate shall mitigate, to the extent practicable, any harmful effect that is known to Business Associate of a use or disclosure of Protected Health Information by Business Associate in violation of the requirements of this Agreement.

d.   **Notice of Use or Disclosure, Security Incident or Breach.** Business Associate shall notify Metro of any use or disclosure of PHI by Business Associate not permitted by this Agreement, any Security Incident (as defined in 45 C.F.R. section 164.304) involving Electronic PHI, and any Breach of Protected Health Information within five (5) business days.

(i)   Business Associate shall provide the following information to Metro within ten (10) business days of discovery of a Breach except when despite all reasonable efforts by Business Associate to obtain the information required, circumstances beyond the control of the Business Associate necessitate additional time. Under such circumstances, Business Associate shall provide to Metro the following information as soon as possible and without unreasonable delay, but in no event later than thirty (30) calendar days from the date of discovery of a Breach:

    (1)   The date of the Breach;

    (2)   The date of the discovery of the Breach;

    (3)   A description of the types of PHI that were involved;

    (4)   identification of each individual whose PHI has been, or is reasonably believed to have been, accessed, acquired, or disclosed; and

    (5)   Any other details necessary to complete an assessment of the risk of harm to the Individual.

(ii)   Business Associate shall cooperate with Metro in investigating the security breach and in meeting Metro's notification obligations under the HITECH Act and any other security breach notification laws.

(iii)   Business Associate agrees to pay actual costs for notification after a determination by Metro that the Breach is significant enough to warrant such measures.

(iv)   Business Associate agrees to establish procedures to investigate the Breach, mitigate losses, and protect against any future Breaches, and to provide a description of these procedures and the specific findings of the investigation to Metro in the time and manner reasonably requested by Metro.

(v)   Business Associate shall report to Metro any successful: (1) unauthorized access, use, disclosure, modification, or destruction of Electronic Protected Health Information; and (2) interference with Business Associate's information systems operations, of which Business Associate becomes aware.

e.   **Compliance of Agents.** Business Associate agrees to ensure that any agent, including a subcontractor, to whom it provides Protected Health Information received from, or created or received by Business Associate on behalf of Metro, agrees to the same restrictions and conditions that apply through this Agreement to Business Associate with respect to such information.

f.   **Access**. Business Associate agrees to provide access, at the request of Metro, and in the time and manner designated by Metro, to Protected Health Information in a Designated Record Set, to Metro or, as directed by Metro, to an Individual, so that Metro may meet its access obligations under 45 CFR § 164.524, HIPAA and the HITECH Act.

g.   **Amendments**. Business Associate agrees to make any amendment(s) to Protected Health Information in a Designated Record Set that Metro directs or agrees at the request of Metro or an Individual, and in the time and manner designated by Metro, so that Metro may meet its amendment obligations under 45 CFR § 164.526, HIPAA and the HITECH Act.

h.   **Disclosure of Practices, Books, and Records**. Business Associate shall make its internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by Business Associate on behalf of, Metro available to Metro, or at the request of Metro to the Secretary, in a time and manner designated by Metro or the Secretary, for purposes of determining Metro's compliance with the HIPAA Privacy Regulations.

i.   **Accounting**. Business Associate shall provide documentation regarding any disclosures by Business Associate that would have to be included in an accounting of disclosures to an Individual under 45 CFR § 164.528 (including without limitation a disclosure permitted under 45 CFR § 164.512) and under the HITECH Act. Business Associate shall make the disclosure Information available to Metro within thirty (30) days of Metro's request for such disclosure Information to comply with an individual's request for disclosure accounting. If Business Associate is contacted directly by an individual based on information provided to the individual by Metro and as required by HIPAA, the HITECH Act or any accompanying regulations, Business Associate shall make such disclosure Information available directly to the individual.

j.   **Security of Electronic Protected Health Information.** Business Associate agrees to: (1) implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the Electronic Protected Health Information that it creates, receives, maintains or transmits on behalf of Metro; (2) ensure that any agent, including a subcontractor, to whom it provides such information agrees to implement reasonable and appropriate safeguards to protect it; and (3) report to Metro any security incident of which it becomes aware.

k.   **Minimum Necessary**. Business Associate agrees to limit its uses and disclosures of, and requests for, PHI: (a) when practical, to the information making up a Limited Information Set; and (b) in all other cases subject to the requirements of 45 CFR 164.502(b), to the minimum amount of PHI necessary to accomplish the intended purpose of the use, disclosure or request.

l.   **Compliance with HITECH Standards.** Business Associate shall comply with the HITECH Standards as specified by law.

m.   **Compliance with Electronic Transactions and Code Set Standards**: If Business Associate conducts any Standard Transaction for, or on behalf, of Metro, Business Associate shall comply, and shall require any subcontractor or agent conducting such Standard Transaction to comply, with each applicable requirement of Title 45, Part 162 of the Code of Federal Regulations. Business Associate shall not enter into, or permit its subcontractor or agents to enter into, any Agreement in connection with

the conduct of Standard Transactions for or on behalf of Metro that:

(i)   Changes the definition, Health Information condition, or use of a Health Information element or segment in a Standard;

(ii)   Adds any Health Information elements or segments to the maximum defined Health Information Set;

(iii)   Uses any code or Health Information elements that are either marked "not used" in the Standard's Implementation Specification(s) or are not in the Standard's Implementation Specifications(s); or

(iv)   Changes the meaning or intent of the Standard's Implementations Specification(s).

n.   **Indemnity.** Business Associate shall indemnify and hold harmless Metro, its officers, agents and employees from and against any claim, cause of action, liability, damage, cost or expense, including attorneys' fees, arising out of or in connection with any non-permitted use or disclosure of Protected Health Information or other breach of this Agreement by Business Associate or any subcontractor or agent of the Business Associate.

SECTION 3 - OBLIGATIONS OF METRO

a.   Metro shall notify Business Associate of any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, to the extent that such changes may affect Business Associate's use or disclosure of Protected Health Information.

b.   Metro shall notify Business Associate of any restriction to the use or disclosure of Protected Health Information that Metro has agreed to in accordance with 45 CFR § 164.522, to the extent that such restriction may affect Business Associate's use or disclosure of Protected Health Information.

SECTION 4 – TERM, TERMINATION AND RETURN OF PHI

a.   **Term**. The Term of this Agreement shall be effective when file in the office of the Metropolitan Clerk and shall terminate when all of the Protected Health Information provided by Metro to Business Associate, or created or received by Business Associate on behalf of Metro, is destroyed or returned to Metro, or, if it is infeasible to return or destroy Protected Health Information, protections are extended to such information, in accordance with the termination provisions in this section. The maximum length as outlined in the Master Contract Agreement or Purchase Order.

b.   **Termination for Cause.** Upon Metro's knowledge of a material breach by Business Associate, Metro shall provide an opportunity for Business Associate to cure the breach or end the violation. Metro may terminate this Agreement between Metro and Business Associate if Business Associate does not cure the breach or end the violation within fourteen (14) days. In addition, Metro may immediately terminate this Agreement if Business Associate has breached a material term of this Agreement and cure is not feasible.

c.   **Obligations on Termination.**

(i)   Except as provided in subsection (ii), upon termination of this Agreement, for any reason, Business Associate shall return or destroy as determined by Metro, all Protected Health Information received from Metro, or created or received by Business Associate on behalf of Metro. This provision shall apply to Protected Health Information that is in the possession of subcontractor or agents of the Business Associate. Business Associate shall retain no copies of the Protected Health Information. Business Associate shall complete such return or destruction as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement. Within such sixty (60) day period, Business Associate shall certify on oath in writing to Metro that such return or destruction has been completed.

(ii)   In the event that Business Associate determines that returning or destroying the Protected Health Information is infeasible, Business Associate shall provide to Metro notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Parties that return or destruction of Protected Health Information is infeasible, Business Associate shall extend the protections of this Agreement to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return

or destruction infeasible, for so long as Business Associate maintains such Protected Health Information. If Metro does not agree that return or destruction of Protected Health Information is infeasible, subparagraph (i) shall apply. Business Associate shall complete these obligations as promptly as possible, but no later than sixty (60) days following the termination or other conclusion of this Agreement.

SECTION 5 - MISCELLANEOUS

a.   **Regulatory References.** A reference in this Agreement to a section in HIPAA or the HITECH Act means the section as in effect or as amended, and for which compliance is required.

b.   **Amendment.** The Parties agree to take such action as is necessary to amend this Agreement from time to time as is necessary for Metro to comply with the requirements of HIPAA or the HITECH Act and any applicable regulations in regard to such laws.

c.   **Survival.** The respective rights and obligations of Business Associate shall survive the termination of this Agreement.

d.   **Interpretation.** Any ambiguity in this Agreement shall be resolved in favor of a meaning that permits Metro to comply with HIPAA or the HITECH Act or any applicable regulations in regard to such laws.

e.   **Governing Law.** The validity, construction, and effect of this Agreement and any and all extensions and/or modifications thereof shall be governed by the laws of the State of Tennessee. Tennessee law shall govern regardless of any language in any attachment or other document that Business Associate may provide.

f.   **Venue.** Any action between the parties arising from this Agreement shall be maintained in the courts of Davidson County, Tennessee.

SECTION PCI

Payment Card Industry (PCI) Security Standards

1. **Payment application vendor.** Contractor that sells and supports applications that store, process, and/or transmit cardholder data shall have application assessed and validated for compliance with the Payment Application Data Security Standard (PA-DSS). Proof of validation shall be provided.

2. **Payment terminal vendor.** Contractor that sells and supports devices used to accept card payments (e.g., payment terminal) shall have the PIN Transaction Security (PTS) devices validated to conform to the PCI PTS standard.

3. **Payment processors, e-commerce hosting providers/processors.** Contractor that stores, processes, or transmits cardholder data on behalf of Metro or that hosts and manages any e-commerce server/website and/or develop and support Metro websites shall provide a PCI Data Security Standard (PCI DSS) Attestation of Compliance for the contracted service.

4. **Providers of software as a service.** Contractor that develops, hosts and/or manages any Metro cloud-based web application or payment application (e.g., online ticketing or booking application) shall provide a PCI Data Security Standard (PCI DSS) Attestation of Compliance for the contracted service.

5. **Integrators/resellers.** Contractor that installs PA-DSS validated payment applications for Metro must be a PCI Qualified Integrator or Reseller (QIR).

6. All applicable compliance shall be maintained for the duration of the contract. Proof of validation shall be current, valid for the service under contract and available upon request.