


<div><div><b>CONTRACT</b> (state revenue contract with a federal or Tennessee local or quasi-governmental entity)</div></div>			
<b>Begin Date</b> April 1, 2025	<b>End Date</b> March 31, 2030	<b>Agency Tracking #</b> 34320-02325	<b>Edison ID</b>
<b>Procuring Party Legal Entity Name</b> Metropolitan Government of Nashville and Davidson County, Acting By and Through the Metropolitan Board of Health			<b>Procuring Party Registration ID</b> 4
<b>Service Caption</b> Issuance of Vital Records birth and death certificates from the Vital Records Information Systems Management (VRISM).			
<b>Agency Contact &amp; Telephone #</b> Christa Morphew 710 James Robertson Pkwy, 1 <sup>st</sup> FL Nashville, TN 37243 615-741-0352 christa.r.morphew@tn.gov		OCR USE - RV	

**CONTRACT  
BETWEEN THE STATE OF TENNESSEE,  
TENNESSEE DEPARTMENT OF HEALTH  
AND  
METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY, ACTING BY AND  
THROUGH THE METROPOLITAN BOARD OF HEALTH**

This Contract, by and between the State of Tennessee, Department of Health, hereinafter referred to as the "State" and Metropolitan Government of Nashville and Davidson County Acting By and Through the Metropolitan Board of Health, hereinafter referred to as the "Procuring Party," is for the provision of issuance of Vital Records birth and death certificates from the Vital Records Information Systems Management (VRISM), as further defined in the "SCOPE OF SERVICES."

**A. SCOPE OF SERVICES:**

A.1. The Procuring Party shall provide all service and deliverables as required, described, and detailed herein and all service delivery timelines as specified by this contract.

A.2. Definition: For purposes of this Contract, definitions shall be as follows and as set forth in the Contract:

- a.) Network Tennessee (NETTN)- a robust, private wide-area network structure that serves the diverse needs of the state's citizens, governmental entities, from the local level through all three (3) branches of state government, and educational institutions. This network allows communication across buildings, departments, and government branches.
- b.) VRISM- a digital registration and management software system for State of Tennessee vital records.
- c.) FileNet- an image repository where TN vital records are stored and retrieved.

A.3. Service Goals:

Allowing the Procuring Party to access VRISM for the purpose of issuing copies of birth and death certificates.

A.4. Service Recipients:

Service recipients are citizens of the local county area that are looking to obtain a copy of a birth and death certificates.

A.5. Service Description:

- a) The State shall:
  - 1. Allow the Procuring Party to access VRISM for the purpose of issuing copies of birth and death certificates.
  - 2. Maintain VRISM in accordance with procedures established by the State.
  - 3. Provide training and written procedures to the Procuring Party on certificate security, issuance and the operation of the VRISM application.
  - 4. Provide training on the ordering and secure storage of the security paper.
  - 5. Provide security paper to Procuring Party.

6. Provide help desk and support services procedures for VRISM issues during state business hours.
7. Provide security specifications for facilities, NETTN connectivity, terminals, printers, and other equipment using VRISM. The State shall perform unscheduled site visits to verify security compliance of the VRISM database and security paper procedures.

b.) The Procuring Party shall:

1. Maintain the confidentiality of the information received as provided in the Tenn. Code Ann. 68-3-206.
2. Access VRISM and issue copies of the Tennessee birth and death certificates solely in the conduct of its official duties at Metropolitan Government of Nashville and the Davidson County, Acting By and Through the Metropolitan Board of Health.
3. Abide by all procedures and rules for certificate security and issuance and for the operation of VRISM outlined by the State.
4. Monthly, a listing shall be provided to Vital Records which details the number of the first and additional copies of birth and death certificates and voided certificates issued from the VRISM database.
5. Limit access to VRISM to those employees who have successfully completed the system user agreement and training.
6. Always provide security for the equipment used to access VRISM and for the security paper used to provide certified copies of birth and death vital records.
7. Be responsible for expenses necessary for NETTN connectivity, terminals, printers, and other equipment, and secure facilities for the equipment and connectivity connection(s) according to State Specifications.
8. Provide written procedures that detail security specifications compliance as defined in Contract section A.5.(a)(7).
9. Provide all technical support services for the connectivity and equipment. The State agency through which the NETTN connectivity is primarily established is the first point of contact for trouble shooting connectivity issues. The primary support shall transfer all non-connectivity issues, VRISM issues, to the Tennessee Division of Vital Records & Statistics.

A.6. Service Reporting:

Compensation to the State shall be made monthly based upon a listing provided by the Procuring Party which will detail the number of first and additional copies of certificates minus voided certificates from VRISM.

A.7. Service Deliverables:

Deliverables	Contract Section	Delivery Date	Due to Whom?	Requested Format
Allow Procuring Party to access VRISM for the purpose of issuing	A.5.a.(1)	Ongoing	Procuring Party	Electronic

<b>Deliverables</b>	<b>Contract Section</b>	<b>Delivery Date</b>	<b>Due to Whom?</b>	<b>Requested Format</b>
Tennessee birth and death certificates				
Maintain VRISM in accordance with procedures established by the State.	A.5.a.(2)	Ongoing	Procuring Party	Electronic
Provide training and written procedures to the Procuring Party on certificate security and issuance and on the operation of VRISM	A.5.a.(3)	Ongoing	Procuring Party	In person, video conferencing or via an instruction manual
Provide training on the ordering and secure storage of security paper	A.5.a.(4)	At the Effective Date	Procuring Party	In person, video conferencing or via an instruction manual
Provide certificate security paper to Procuring Party.	A.5.a.(5)	Ongoing	Procuring Party	In person, video conferencing or via an instruction manual
Provide support services procedures for VRISM issues	A.5.a.(6)	Ongoing	Procuring Party	To be Determined
Provide security specifications for facilities, <b>NETTN</b> connectivity, terminals, printers, and other equipment using <b>VRISM</b> . The State shall perform unscheduled site visits to verify security compliance.	A.5.a.(7)	At the beginning of the contract and then ongoing	Procuring Party/State	To be Determined
Maintain the confidentiality of the information received as provided in Tenn. Code Ann. 68-3-206	A.5.b.(1)	Ongoing	Procuring Party/State	Internal security procedures from the Procuring Party
Access VRISM and issue copies of birth and death certificates solely in the conduct of its official duties at Metropolitan Government of Nashville and Davidson County, Acting By and Through the Metropolitan Board of Health.	A.5.b.(2)	Ongoing	Customers requesting birth and death vital records certificates in Davidson County.	Sequentially numbered security paper.
Abide by all procedures and rules for certificate security and issuance and for the operation of VRISM outlined by the State	A.5.b.(3)	Ongoing	Procuring Party/State	Internal security procedures
Limited access to VRISM to those employees who have successfully completed the	A.5.b.(4)	Ongoing	Procuring Party/State	Internal security procedures from the Procuring Party

<b>Deliverables</b>	<b>Contract Section</b>	<b>Delivery Date</b>	<b>Due to Whom?</b>	<b>Requested Format</b>
system user agreement and training.				
Provide security at all times for the equipment used for VRISM and for the security paper used to provide certified copies of TN birth and death records. with VRISM.	A.5.b.(5)	Ongoing	Procuring Party/State	Internal security procedures from the Procuring Party
Monthly, a listing shall be provided to the Department which details the number of the first and additional copies of birth and death certificates and voided certificates issued from the VRISM database.	A.5.b.(6)	Ongoing	State	Via Information Technology Services
Be responsible for expenses necessary NETTN connectivity, terminals, printers, and other equipment, and secure facilities for the equipment and connectivity connection(s) according to State specifications.	A.5.b.(7)	Ongoing	State	Via Information Technology Services
Provide written procedures that detail security specifications compliance as defined in Contract section A.5.(a).7.	A.5.b.(8)	At the Effective Date and ongoing	State	Word format in electronic form and booklet form
Provide all technical support services for the connectivity and equipment. The State agency through which the NETTN connectivity is primarily established is the first point of contact for trouble shooting connectivity issues. The primary support shall transfer all non-connectivity issues, VRISM issues, to the State Office of Vital Records	A.5.b.(9)	Ongoing	State	Via Information Technology Services

**B. TERM OF CONTRACT:**

This Contract shall be effective on April 1, 2025 ("Effective Date"), and extend for a period of Sixty (60) months after the Effective Date ("Term"). The State shall have no obligation for goods or

services provided by the Contractor prior to the Effective Date. This Contract may not be extended or renewed.

**C. PAYMENT TERMS AND CONDITIONS:**

- C.1.** The Procuring Party shall retain \$6.50 for the search and copy or copies of all certificates that are issued. The Procuring Party shall compensate the State \$8.50 of fees collected for the search and copy or copies of all certificates that are issued. The current fees to be collected are designated in the Rules of the Tennessee Department of Health, Chapter 1200-7-1-.13, Fees for Copies and Searches.
- C.2** Compensation to the State shall be made monthly based upon a listing provided by the State which will detail the number of first and additional copies of certificates minus voided certificates issued from the database.
- C.3** The compensation to the State as described in Section C is for the duration of the Contract and is not subject to escalation for any reason, unless amended.

**D. STANDARD TERMS AND CONDITIONS:**

- D.1.** Required Approvals. The State is not bound by this Contract until it is signed by the contract parties and approved by appropriate officials in accordance with applicable Tennessee laws and regulations (depending upon the specifics of this contract, said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).
- D.2.** Modification and Amendment. This Contract may be modified only by a written amendment signed by all parties hereto and approved by both the officials who approved the base contract and, depending upon the specifics of the contract as amended, any additional officials required by Tennessee laws and regulations (said officials may include, but are not limited to, the Commissioner of Finance and Administration, the Commissioner of Human Resources, and the Comptroller of the Treasury).
- D.3.** Termination for Convenience. The Contract may be terminated by either party by giving written notice to the other, at least thirty (30) days before the effective date of termination. Said termination shall not be deemed a Breach of Contract by the State. Should the State exercise this provision, the State shall have no liability to the Procuring Party. Should either the State or the Procuring Party exercise this provision, the Procuring Party shall be required to compensate the State for satisfactory, authorized services completed as of the termination date and shall have no liability to the State except for those units of service which can be effectively used by the Procuring Party. The final decision, as to what these units of service are, shall be determined by the State. In the event of disagreement, the Procuring Party may file a claim with the Tennessee Claims Commission in order to seek redress.
- Upon such termination, the Procuring Party shall have no right to any actual general, special, incidental, consequential, or any other damages whatsoever of any description or amount.
- D.4.** Termination for Cause. If either party fails to properly perform or fulfill its obligations under this Contract in a timely or proper manner or violates any terms of this Contract, the other party shall have the right to immediately terminate the Contract. The Procuring Party shall compensate the State for completed services.
- D.5.** Subcontracting. Neither the Procuring Party nor the State shall assign this Contract or enter into a subcontract for any of the services performed under this Contract without obtaining the prior

written approval of the other. If such subcontracts are approved, they shall contain, at a minimum, sections of this Contract below pertaining to "Conflicts of Interest," "Nondiscrimination," and "Records" (as identified by the section headings).

- D.6. Conflicts of Interest. The Procuring Party warrants that no amount shall be paid directly or indirectly to an employee or official of the State of Tennessee as wages, compensation, or gifts in exchange for acting as an officer, agent, employee, subcontractor, or consultant to the Procuring Party in connection with any work contemplated or performed relative to this Contract other than as required by section A. of this Contract.
- D.7. Nondiscrimination. The State and the Procuring Party hereby agree, warrant, and assure that no person shall be excluded from participation in, be denied benefits of, or be otherwise subjected to discrimination in the performance of this Contract or in the employment practices of the State or the Procuring Party on the grounds of handicap or disability, age, race, color, religion, sex, national origin, or any other classification protected by Federal, Tennessee State constitutional, or statutory law.
- D.8. Records. The Procuring Party shall maintain documentation for its transactions with the State under this Contract. The books, records, and documents of the Procuring Party, insofar as they relate to work performed or money paid under this Contract, shall be maintained for a period of five (5) full years from the final date of this Contract and shall be subject to audit, at any reasonable time and upon reasonable notice, by the state agency, the Comptroller of the Treasury, or their duly appointed representatives. The financial statements shall be prepared in accordance with generally accepted accounting principles.
- D.9. Strict Performance. Failure by any party to this Contract to insist in any one or more cases upon the strict performance of any of the terms, covenants, conditions, or provisions of this Contract shall not be construed as a waiver or relinquishment of any such term, covenant, condition, or provision. No term or condition of this Contract shall be held to be waived, modified, or deleted except by a written amendment signed by the parties hereto.
- D.10. Independent Contractor. The parties hereto, in the performance of this Contract, shall not act as employees, partners, joint venturers, or associates of one another. It is expressly acknowledged by the parties hereto that such parties are independent contracting entities and that nothing in this Contract shall be construed to create an employer/employee relationship or to allow either to exercise control or direction over the manner or method by which the other transacts its business affairs or provides its usual services. The employees or agents of one party shall not be deemed or construed to be the employees or agents of the other party for any purpose whatsoever.
- D.11. State Liability. The State shall have no liability except as specifically provided in this Contract.
- D.12. Force Majeure. The obligations of the parties to this Contract are subject to prevention by causes beyond the parties' control that could not be avoided by the exercise of due care including, but not limited to, natural disasters, riots, wars, epidemics, or any other similar cause.
- D.13. State and Federal Compliance. The Procuring Party and the State shall comply with all applicable State and Federal laws and regulations in the performance of this Contract.
- D.14. Governing Law. This Contract shall be governed by and construed in accordance with the laws of the State of Tennessee. The Procuring Party agrees that it will be subject to the exclusive jurisdiction of the courts of the State of Tennessee in actions that may arise under this Contract. The Procuring Party acknowledges and agrees that any rights or claims against the State of Tennessee or its employees hereunder, and any remedies arising therefrom, shall be subject to and limited to those rights and remedies, if any, available under *Tennessee Code Annotated*, Sections 9-8-101 through 9-8-407.



- D.15. Completeness. This Contract is complete and contains the entire understanding between the parties relating to the subject matter contained herein, including all the terms and conditions of the parties' agreement. This Contract supersedes any and all prior understandings, representations, negotiations, and agreements between the parties relating hereto, whether written or oral.
- D.16. Severability. If any terms and conditions of this Contract are held to be invalid or unenforceable as a matter of law, the other terms and conditions hereof shall not be affected thereby and shall remain in full force and effect. To this end, the terms and conditions of this Contract are declared severable.
- D.17. Headings. Section headings of this Contract are for reference purposes only and shall not be construed as part of this Contract.
- D.18. Confidentiality of Records. Strict standards of confidentiality of records and information shall be maintained in accordance with applicable state and federal law. All material and information, regardless of form, medium or method of communication, provided to the Contractor by the State or acquired by the Contractor on behalf of the State that is regarded as confidential under state or federal law shall be regarded as "Confidential Information." Nothing in this Section shall permit Contractor to disclose any Confidential Information, regardless of whether it has been disclosed or made available to the Contractor due to intentional or negligent actions or inactions of agents of the State or third parties. Confidential Information shall not be disclosed except as required or permitted under state or federal law. Contractor shall take all necessary steps to safeguard the confidentiality of such material or information in conformance with applicable state and federal law. The obligations set forth in this Section shall survive the termination of this Contract.

**E. SPECIAL TERMS AND CONDITIONS:**

- E.1. Conflicting Terms and Conditions. Should any of these special terms and conditions conflict with any other terms and conditions of this Contract, these special terms and conditions shall control.
- E.2. Communications and Contacts. All instructions, notices, consents, demands, or other communications required or contemplated by this Contract shall be in writing and shall be made by certified, first-class mail, return receipt requested and postage prepaid, by overnight courier service with an asset tracking system, or by EMAIL or facsimile transmission with recipient confirmation. Any such communications, regardless of method of transmission, shall be addressed to the respective party at the appropriate mailing address, facsimile number, or EMAIL address as set forth below or to that of such other party or address, as may be hereafter specified by written notice.

The State:

Edward G. Bishop  
Tennessee Department of Health  
Division of Vital Records & Statistics  
710 James Robertson Parkway  
1<sup>st</sup> Floor, Andrew Johnson Tower  
Nashville, TN 37243  
Gray.Bishop@tn.gov  
Telephone # 615-532-2600

The Procuring Party:

Sanmi Areola, Director  
Metropolitan Public Health Department  
2500 Charlotte Avenue



Nashville, TN 37209  
Sanmi.areola@nashville.gov  
Telephone # 615-340-5622

All instructions, notices, consents, demands, or other communications shall be considered effectively given upon receipt or recipient confirmation as may be required.

- E.3. HIPAA Compliance. The State and Procuring Party shall comply with obligations under the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and its accompanying regulations.
- a. Procuring Party warrants to the State that it is familiar with the requirements of HIPAA and its accompanying regulations and will comply with all applicable HIPAA requirements in the course of this Contract.
  - b. Procuring Party warrants that it will cooperate with the State, including cooperation and coordination with State privacy officials and other compliance officers required by HIPAA and its regulations, in the course of performance of the Contract so that both parties will be in compliance with HIPAA.
  - c. The State and the Procuring Party will sign documents, including but not limited to business associate agreements, as required by HIPAA and that are reasonably necessary to keep the State and Procuring Party in compliance with HIPAA. This provision shall not apply if information received by the State under this Contract is NOT "protected health information" as defined by HIPAA, or if HIPAA permits the State to receive such information without entering into a business associate agreement or signing another such document.
- E.4. State Furnished Property. The Procuring Party shall be responsible for the correct use, maintenance, and protection of all articles of nonexpendable, tangible, personal property furnished by the State for the Procuring Party's temporary use under this Contract. Upon termination of this Contract, all property furnished shall be returned to the State in good order and condition as when received, reasonable use and wear thereof excepted. Should the property be destroyed, lost, or stolen, the Procuring Party shall be responsible to the State for the residual value of the property at the time of loss.
- E.5. Personally Identifiable Information. While performing its obligations under this Contract, Contractor may have access to Personally Identifiable Information held by the State ("PII"). For the purposes of this Contract, "PII" includes "Nonpublic Personal Information" as that term is defined in Title V of the Gramm-Leach-Bliley Act of 1999 or any successor federal statute, and the rules and regulations thereunder, all as may be amended or supplemented from time to time ("GLBA") and personally identifiable information and other data protected under any other applicable laws, rule or regulation of any jurisdiction relating to disclosure or use of personal information ("Privacy Laws"). Contractor agrees it shall not do or omit to do anything which would cause the State to be in breach of any Privacy Laws. Contractor shall, and shall cause its employees, agents and representatives to: (i) keep PII confidential and may use and disclose PII only as necessary to carry out those specific aspects of the purpose for which the PII was disclosed to Contractor and in accordance with this Contract, GLBA and Privacy Laws; and (ii) implement and maintain appropriate technical and organizational measures regarding information security to: (A) ensure the security and confidentiality of PII; (B) protect against any threats or hazards to the security or integrity of PII; and (C) prevent unauthorized access to or use of PII. Contractor shall immediately notify State: (1) of any disclosure or use of any PII by Contractor or any of its employees, agents and representatives in breach of this Contract; and (2) of any disclosure of any PII to Contractor or its employees, agents and representatives where the purpose of such disclosure is not known to Contractor or its employees, agents and representatives. The State reserves the right to review Contractor's policies and procedures used to maintain the security and confidentiality of PII and Contractor shall, and cause its employees, agents and representatives to, comply with all reasonable requests or directions from the State to enable the State to verify or ensure that

Contractor is in full compliance with its obligations under this Contract in relation to PII. Upon termination or expiration of the Contract or at the State's direction at any time in its sole discretion, whichever is earlier, Contractor shall immediately return to the State any and all PII which it has received under this Contract and shall destroy all records of such PII.

The Contractor shall report to the State any instances of unauthorized access to or potential disclosure of PII in the custody or control of Contractor ("Unauthorized Disclosure") that come to the Contractor's attention. Any such report shall be made by the Contractor within twenty-four (24) hours after the Unauthorized Disclosure has come to the attention of the Contractor. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures. The Contractor, at the sole discretion of the State, shall provide no cost credit monitoring services for individuals whose PII was affected by the Unauthorized Disclosure. The Contractor shall bear the cost of notification to all individuals affected by the Unauthorized Disclosure, including individual letters and public notice. The remedies set forth in this Section are not exclusive and are in addition to any claims or remedies available to this State under this Contract or otherwise available at law. The obligations set forth in this Section shall survive the termination of this Contract.

**E.6. Information Technology Security Requirements (State Data, Audit, and Other Requirements).**

a. The Contractor shall protect State Data as follows:

- (1) The Contractor shall ensure that all State Data is housed in the continental United States, inclusive of backup data. All State data must remain in the United States, regardless of whether the data is processed, stored, in-transit, or at rest. Access to State data shall be limited to US-based (onshore) resources only.

All system and application administration must be performed in the continental United States. Configuration or development of software and code is permitted outside of the United States. However, software applications designed, developed, manufactured, or supplied by persons owned or controlled by, or subject to the jurisdiction or direction of, a foreign adversary, which the U.S. Secretary of Commerce acting pursuant to 15 CFR 7 has defined to include the People's Republic of China, among others are prohibited. Any testing of code outside of the United States must use fake data. A copy of production data may not be transmitted or used outside the United States.

- (2) The Contractor shall encrypt Confidential State Data at rest and in transit using the current version of Federal Information Processing Standard ("FIPS") 140-2 or 140-3 (or current applicable version) validated encryption technologies.
- (3) The Contractor shall implement and maintain privacy and security controls that follow the guidelines set forth in NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," or NIST 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," as amended from time to time. Contractor shall meet annually, or as otherwise agreed, with the State to review the implementation of this Section. A "System Security Plan (SSP)" is required regardless of the type of third-party Controls Audit the Contractor obtains.

No additional funding shall be allocated for these examinations as they are included in the Maximum Liability of this Contract.

- (4) The Contractor must annually perform Penetration Tests and Vulnerability Assessments against its Processing Environment per the NIST 800-115 definition. "Processing Environment" shall mean the combination of software and hardware on which the Application runs. "Application" shall mean the computer code that supports and accomplishes the State's requirements as set forth in this Contract. "Penetration Tests" shall be in the form of attacks on the Contractor's computer system, with the purpose of discovering security weaknesses

which have the potential to gain access to the Processing Environment's features and data. The "Vulnerability Assessment" shall be designed and executed to define, identify, and classify the security holes (vulnerabilities) in the Processing Environment. The Contractor shall provide a letter of attestation on its processing environment that penetration tests and vulnerability assessments has been performed on an annual basis and taken corrective action to evaluate and address any findings. The Contractor must provide a letter of attestation that includes a penetration testing and vulnerability assessments report that outlines risk exposure of the critical, high, and moderate risks and how they were mitigated, within 30 days of receiving the results.

In the event of an unauthorized disclosure or unauthorized access to State data, the State Strategic Technology Solutions (STS) Security Incident Response Team (SIRT) must be notified and engaged by calling the State Customer Care Center (CCC) at 615-741-1001. Any such event must be reported by the Contractor within twenty-four (24) hours after the unauthorized disclosure has come to the attention of the Contractor.

- (5) If a breach has been confirmed a fully un-modified third-party forensics report must be supplied to the State and through the STS SIRT. This report must include indicators of compromise (IOCs) as well as plan of actions for remediation and restoration. Contractor shall take all necessary measures to halt any further Unauthorized Disclosures.
- (6) Upon State request, the Contractor shall provide a copy of all Confidential State Data it holds. The Contractor shall provide such data on media and in a format determined by the State
- (7) Upon termination of this Contract and in consultation with the State, the Contractor shall destroy, and ensure all subcontractors shall destroy, all Confidential State Data it holds (including any copies such as backups) in accordance with the current version of National Institute of Standards and Technology ("NIST") Special Publication 800-88. The Contractor shall provide a written confirmation of destruction to the State within ten (10) business days after destruction.

b. Minimum Requirements

- (1) The Contractor and all data centers used by the Contractor to host State data, including those of all Subcontractors, must comply with the most current version of NIST 800-53, "Security and Privacy Controls for Federal Information Systems and Organizations," or NIST 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," with the State to review the implementation of this Section. The State must have proof of compliance with NIST 800-53 or NIST 800-171 in the form of a third-party audit at a minimum every two years or upon request. Davidson County Information Security Management Policies are located at: <https://www.nashville.gov/departments/information-technology-services/information-security/information-security-policies>
- (2) The Contractor agrees to maintain the Application so that it will run on a current, manufacturer-supported Operating System. "Operating System" shall mean the software that supports a computer's basic functions, such as scheduling tasks, executing applications, and controlling peripherals.
- (3) If the Application requires middleware or database software, Contractor shall maintain middleware and database software versions that are always fully compatible with current versions of the Operating System and Application to ensure that security vulnerabilities are not introduced.
- (4) In the event of drive/media failure, if the drive/media is replaced, it remains with the State and it is the State's responsibility to destroy the drive/media, or the Contractor shall provide written confirmation of the sanitization/destruction of data according to NIST 800-88.

- c. **Business Continuity Requirements.** The Contractor shall maintain set(s) of documents, instructions, and procedures which enable the Contractor to respond to accidents, disasters, emergencies, or threats without any stoppage or hindrance in its key operations ("Business Continuity Requirements"). Business Continuity Requirements shall include:
  - (1) "Disaster Recovery Capabilities" refer to the actions the Contractor takes to meet the Recovery Point and Recovery Time Objectives defined below. Disaster Recovery Capabilities shall meet the following objectives:
    - i. **Recovery Point Objective ("RPO").** The RPO is defined as the maximum targeted period in which data might be lost from an IT service due to a major incident: 1 hour
    - ii. **Recovery Time Objective ("RTO").** The RTO is defined as the targeted duration of time and a service level within which a business process must be restored after a disaster (or disruption) in order to avoid unacceptable consequences associated with a break in business continuity: 24 hours
  - (2) The Contractor and the Subcontractor(s) shall maintain a documented Disaster Recovery plan and shall share this document with the State when requested. The Contractor and the Subcontractor(s) shall perform at least one Disaster Recovery Test every three hundred sixty-five (365) days. A "Disaster Recovery Test" shall mean the process of verifying the success of the restoration procedures that are executed after a critical IT failure or disruption occurs. The Disaster Recovery Test shall use actual State Data Sets that mirror production data, and success shall be defined as the Contractor verifying that the Contractor can meet the State's RPO and RTO requirements. A "Data Set" is defined as a collection of related sets of information that is composed of separate elements but can be manipulated as a unit by a computer. The Contractor shall provide written confirmation to the State after each Disaster Recovery Test that its Disaster Recovery Capabilities meet the RPO and RTO requirements.

#### E.7. Comptroller Audit Requirements.

When requested by the State or the Comptroller of the Treasury, the Contractor must provide the State or the Comptroller of the Treasury with a detailed written description of the Contractor's information technology control environment, including a description of general controls and application controls. The Contractor must also assist the State or the Comptroller of the Treasury with obtaining a detailed written description of the information technology control environment for any third or fourth parties, or Subcontractors, used by the Contractor to process State data and/or provide services under this Grant.

Contractor will maintain and cause its Subcontractors to maintain a complete audit trail of all transactions and activities in connection with this Grant, including all information technology logging and scanning conducted within the Contractor's and Subcontractor's information technology control environment. Upon reasonable notice and at any reasonable time, the Contractor grants the State or the Comptroller of the Treasury with the right to audit the Contractor's information technology control environment, including general controls and application controls. The audit may include testing the general and application controls within the Contractor's information technology control environment and may also include testing general and application controls for any third or fourth parties, or Subcontractors, used by the Contractor to process State data and/or provide services under this Grant. The audit may include the Contractor's and Subcontractor's compliance with NIST 800-53 or 800-171 and all applicable requirements, laws, regulations, or policies.

Upon reasonable notice and at any reasonable time, the Contractor and Subcontractor(s) agree to allow the State, the Comptroller of the Treasury, or their duly appointed representatives to perform information technology control audits of the Contractor and all Subcontractors used by the Contractor. Contractor will provide to the State, the Comptroller of the Treasury, or their duly appointed representatives access to Contractor and Subcontractor(s) personnel for the purpose of performing the information technology control audit. The audit may include interviews with technical and management personnel, physical or virtual inspection of controls, and review of paper or electronic documentation.

The Contractor must have a process for correcting control deficiencies that were identified in the State's or Comptroller of the Treasury's information technology audit. For any audit issues identified, the Contractor and Subcontractor(s) shall submit a corrective action plan to the State or the Comptroller of the Treasury which addresses the actions taken, or to be taken, and the anticipated completion date in response to each of the audit issues and related recommendations of the State or the Comptroller of the Treasury. The corrective action plan shall be provided to the State or the Comptroller of the Treasury upon request from the State or Comptroller of the Treasury and within 30 days from the issuance of the audit report or communication of the audit issues and recommendations. Upon request from the State or Comptroller of the Treasury, the Contractor and Subcontractor(s) shall provide documentation and evidence that the audit issues were corrected.




Each party shall bear its own expenses incurred while conducting the information technology controls audit.

**IN WITNESS WHEREOF, the parties have by their duly authorized representatives set their signatures.**

**METROPOLITAN GOVERNMENT OF NASHVILLE AND DAVIDSON COUNTY**

Signed by:		
		3/31/2025
0872295CD81A4B1...		
<b>Director, Metro Public Health Department</b>		<b>Date</b>
Signed by:		
		3/31/2025
BEBF0BBF14D14B0...		
<b>Chair, Board of Health</b>		<b>Date</b>

**APPROVED AS TO AVAILABILITY OF FUNDS:**

Signed by:		Initial	DS	
				3/31/2025
62377A2A8742469...				
<b>Director, Department of Finance</b>				<b>Date</b>

**APPROVED AS TO RISK AND INSURANCE:**

DocuSigned by:		
		4/1/2025
68804BF12FD741C...		

**Date**

4/2/2025

Date \_\_\_\_\_

Date \_\_\_\_\_

Date \_\_\_\_\_