

FRAMEWORK AGREEMENT

THIS FRAMEWORK AGREEMENT (this “Agreement”) is made between the **CITY AND COUNTY OF DENVER**, a municipal corporation of the State of Colorado (the “City”), and **SECURUS TECHNOLOGIES, LLC**, a Delaware limited liability company, whose address is 5360 Legacy Drive, Suite 300, Plano, TX 75024 (the “Contractor”), individually a “Party” and collectively the “Parties.”

RECITALS

WHEREAS, the City awarded this Agreement to the Contractor through a competitive selection and the City’s Executive Order 8 to manage telecommunications at the City’s detention facilities.

NOW, THEREFORE, in consideration of the mutual covenants and agreements hereinafter set forth and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties incorporate the recitals set forth above agree as follows:

1. **COORDINATION AND LIAISON**: The Contractor shall fully coordinate all Work under this Agreement with the City’s Executive Director (“Director”) of the City’s Department of Public Safety or other designated personnel of the Department of Public Safety (“Agency” or “DPS”). For all technology matters, the Contractor shall coordinate with the City’s Chief Information Officer (“CIO”) or other designated personnel of the Department of Technology Services (“TS”).
2. **DEFINITIONS**
 - 2.1. **“City Data”** means all information processed or stored on computers or other electronic media by the City or on the City’s behalf or provided to the Contractor for such processing or storage, as well as any information derived from such information. City Data includes, without limitation: (i) information on paper or other non-electronic media provided to the Contractor for computer processing or storage, or information formerly on electronic media; (ii) information provided to the Contractor by the City, other users, or by other third parties; and (iii) personally identifiable information, confidential or sensitive information, or other regulated data from such users or other third parties, including from the City’s employees.
 - 2.2. **“D(d)ata”** means information, regardless of form, that can be read, transmitted, or processed.
 - 2.3. **“Deliverable(s)”** means a tangible object, SaaS, or On-Premise Software that is provided to the City by the Contractor under this Agreement.
 - 2.4. **“Effective Date”** means the date on which this Agreement is approved and signed by the City as shown on the City’s signature page.
 - 2.5. **“Exhibits”** means the exhibits and attachments included with this Agreement.
 - 2.6. **“On-Premise Software”** means software that the Contractor provides for the City’s use. For the avoidance of doubt, On-Premise Software does not include SaaS, though On-Premise Software may interface with SaaS.
 - 2.7. **“SaaS”** means a software-as-a-service that the Contractor hosts (directly or indirectly) for the City’s use. For the avoidance of doubt, SaaS does not include Services or On-Premise Software.
 - 2.8. **“Service(s)”** means the technology related professional services to be performed by the Contractor as set forth in this Agreement and shall include any services or support provided by the Contractor under this Agreement.
 - 2.9. **“Specifications”** refers to such technical and functional specifications for On-Premise Software,

SaaS, and/or Deliverables included or referenced in an Exhibit.

2.10. “Subcontractor” means any third party engaged by the Contractor to aid in performance of the Work.

2.11. “Task Order” means a document issued in accordance with this Agreement that specifically describes the Work to be performed.

2.12. “Work” means the On-Premise Software, SaaS, Services, hardware, or Deliverables provided and/or performed pursuant to this Agreement.

3. SOFTWARE AS A SERVICE, SUPPORT, AND SERVICES TO BE PERFORMED: As agreed to between the Parties, the Contractor shall diligently undertake, perform, and make available the technology related Work set forth in the Exhibits according to industry standards. The City shall have no liability to compensate the Contractor for Work that is not specifically authorized by this Agreement. The Work shall be provided and performed as stated herein and shall conform to the Specifications. The Contractor is ready, willing, and able to provide the Work required by this Agreement. The Contractor shall faithfully perform any Services in accordance with the standards of care, skill, training, diligence, and judgment provided by highly competent individuals performing services of a similar nature to those described in this Agreement and in accordance with the terms of this Agreement.

4. TASK ORDERS FOR ADDITIONAL PRODUCTS AND SERVICES

4.1. To initiate a Task Order, the City will provide a request to the Contractor describing the general scope and intent of the Work it desires the Contractor to perform under that Task Order. The Contractor shall submit a proposal, which shall include a quote, to the City in response to the City’s request. All Task Orders, signed by the Parties, shall be issued in accordance with this Agreement using the rates contained therein. Each Task Order shall include a detailed scope of Services, level of effort, timeline for completion, rates or fixed fee pricing, and payment schedule, including a “not to exceed” amount, specific to each Task Order. Task Orders shall be construed to be in addition to, supplementary to, and consistent with the provisions of this Agreement. In the event of a conflict between a particular provision of any Task Order and a provision of this Agreement, this Agreement shall take precedence. A Task Order may be amended by the Parties by a written instrument prepared by the Parties jointly and signed by their authorized representatives.

4.2. The City is not required to execute any minimum number of Task Orders under this Agreement, and the City reserves the right to execute Task Orders with the Contractor at its sole discretion. The City shall have no liability to compensate the Contractor for any Work not specifically set forth in this Agreement or a properly executed Task Order. In no event shall a Task Order term extend beyond the Term unless the City has specifically agreed in writing. If this Agreement is terminated for any reason, each Task Order hereunder shall also terminate unless the Parties agree otherwise in writing. Task Orders may also be terminated in accordance with this Agreement’s termination provisions. The Contractor agrees to fully coordinate its provision of Services with any third party under contract with the City doing work or providing Services which affect the Contractor’s performance.

- 4.3. The Contractor represents and warrants that all Services under a Task Order will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards; all Services and/or Deliverables will conform to applicable, agreed upon specifications, if any; and, it has the requisite ownership, rights and licenses to perform its obligations under this Agreement fully as contemplated hereby and to grant to the City all rights with respect to any software and Services free and clear from any and all liens, adverse claims, encumbrances and interests of any third party.
5. **TERM**: This Agreement will commence on March 15, 2025, and will expire, unless sooner terminated, on March 15, 2030 (the “Term”). Subject to the City’s prior written authorization, the Contractor shall complete any Work in progress as of the expiration date and the Term will extend until the work is completed or earlier terminated by the City.
6. **END OF TERM EXTENSION**: If this Agreement approaches the end of its Term, the City, at its discretion and upon written notice to the Contractor as provided herein, may unilaterally extend the Term for a period not to exceed six months (an “End of Term Extension). The provisions of this Agreement and the pricing in effect when such notice is given shall remain in effect during the End of Term Extension. The End of Term Extension shall automatically terminate upon execution of a replacement contract or modification extending this Agreement. To facilitate any agreed upon extensions in a timely manner, the Contractor shall negotiate any extension of this Agreement in good faith and provide the City all required order forms and updated pricing information to the City no later than one hundred twenty (120) days prior to the expiration of the Term. If the Contractor does not intend to extend the Term of this Agreement, the Contractor shall provide prompt notice to the City but not later than one hundred eighty (180) days prior to the expiration of the Term of its intent to let this Agreement lapse without an extension or replacement contract. The Contractor’s obligation to facilitate a timely renewal under this Section is a material part of this Agreement.
7. **COMPENSATION AND PAYMENT**
- 7.1. **Fees**: The City shall pay, and the Contractor shall accept as the sole compensation for Services rendered and costs incurred under this Agreement the fees described in the attached Exhibits, plus applicable taxes and fees. The City will provide Contractor with its tax-exempt certificate upon request. Amounts billed may not exceed rates set forth in the Exhibits and will be made in accordance with any agreed upon payment milestones.
- 7.2. **Reimbursement Expenses**: There are no reimbursable expenses allowed under this Agreement. All the Contractor’s expenses are contained in the budget as described in the Exhibits. The City will not be obligated to pay the Contractor for any other fees, costs, expenses, or charges of any nature that may be incurred and paid by the Contractor in performing their obligations under this Agreement including but not limited to personnel costs, benefits, contract labor, overhead, administrative costs, operating costs, supplies, equipment, and out-of-pocket expenses.
- 7.3. **Invoicing**: The Contractor must submit an invoice which shall include the City contract number, clear identification of the Work that has been completed or delivered, and other information reasonably requested by the City. Invoices are due and payable 30 days from invoice date, provided that payment on all uncontested amounts shall be made in accordance with the City’s

Prompt Payment Ordinance, §§ 20-107, *et seq.*, D.R.M.C, and no Exhibit or order form shall modify the City's statutory payment provisions. Any revenue or commission payments due to the City as described in the Exhibits shall be made in accordance with terms set forth in this Agreement. To the extent permitted by applicable law and regulation, the Contractor reserves the right to propose an increase to the prices in the Agreement on an annual basis by the percentage increase in consumer prices for services during the applicable trailing 12-month period as measured by the United States Consumer Price Index or a similar index should such index no longer be published. Notwithstanding the foregoing limitation on price increases, the Contractor reserves the right to increase prices upon 30 days' notice in the event of a cost increase that exceeds 3% of Contractor's current costs directly related to the Work under this Agreement. All price increases must be agreed to by the Parties in writing. If the City does not agree to the proposed increase, the City may terminate this Agreement.

7.4. Maximum Contract Amount

7.4.1. Notwithstanding any other provision of this Agreement, the City's maximum payment obligation will not exceed Two Million Six Thousand Seven Hundred Eighty Dollars (\$2,006,780.00) (the "Maximum Agreement Amount"). The City is not obligated to execute an Agreement or any amendments for any further Work, including any Services performed by the Contractor beyond that specifically described in the attached Exhibits. Any Work performed beyond those in the attached Exhibits are performed at the Contractor's risk and without authorization under this Agreement.

7.4.2. The City's payment obligation, whether direct or contingent, extends only to funds appropriated annually by the Denver City Council, paid into the Treasury of the City, and encumbered for the purpose of this Agreement. The City does not by this Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. This Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

8. TAXES, CHARGES AND PENALTIES: The City shall not be liable for the payment of taxes, late charges, or penalties of any nature other than the compensation stated herein, except for any additional amounts which the City may be required to pay under D.R.M.C. § 20-107 to § 20-115.

9. STATUS OF CONTRACTOR: The Contractor is an independent contractor retained to perform professional or technical services for limited periods of time. Neither the Contractor nor any of its employees are employees or officers of the City under Chapter 18 of the Denver Revised Municipal Code, or for any purpose whatsoever. Nothing contained in this Agreement shall be construed as creating any agency, partnership, joint venture, or other form of joint enterprise, or employment relationship between the Parties.

10. TERMINATION

10.1. Either Party may terminate this Agreement, and the City may terminate a Work under this Agreement, for the other Party's material breach by written notice specifying in detail the nature of the breach, allowing the other Party the opportunity to cure the breach within thirty (30) days, unless the other Party first cures such breach, or effective immediately if the breach is not subject

to cure. Nothing gives the Contractor the right to perform under this Agreement beyond the time when its Work becomes unsatisfactory to the City.

10.2. The City has the right to terminate this Agreement or a Work under this Agreement without cause upon thirty (30) days prior written notice to the Contractor. If the City terminates this Agreement without cause, the City shall pay for Work due and payable including, but not limited to, installation costs actually incurred where the installation was initiated but not completed. The City is under no obligation to make further payment(s) for any remaining subscription years, licensing fees, or support costs as outlined in the attached Exhibits once the then current annual term expires; provide that, the City shall not be entitled to any refund, unless stated otherwise in the Exhibits, for the remainder of the prepaid annual term then in effect at the time of this Agreement's early termination without cause.

10.3. Notwithstanding the preceding paragraph, the City may terminate this Agreement if the Contractor or any of its officers or employees are convicted, plead nolo contendere, enter into a formal agreement in which they admit guilt, enter a plea of guilty or otherwise admit culpability to criminal offenses of bribery, kickbacks, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with the Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

10.4. Upon termination of this Agreement, with or without cause, the Contractor shall have no claim against the City by reason of, or arising out of, incidental or relating to termination, except for compensation for Work duly requested and performed. Upon the City's request or upon termination, the Contractor shall return to the City all City property placed in the Contractor's possession or control pursuant to this Agreement.

10.5. The City is entering into this Agreement to serve the public interest of the City as determined by its governing bodies. If this Agreement ceases to further the public interest of the City, or if the City fails to appropriate the necessary funding to continue this Agreement, the City, in its discretion, may terminate this Agreement in whole or in part by providing reasonable prior written notice. A determination that this Agreement should be terminated in the public interest or for lack of appropriation shall not be equivalent to a City right to terminate for convenience or without cause. This Subsection shall not apply to a termination of this Agreement by the City for a breach of contract by the Contractor. If the City terminates this Agreement in the public interest or for lack of appropriation, the City shall pay the Contractor an amount equal to the percentage of the total reimbursement payable under this Agreement that corresponds to the percentage of Work performed, as reasonably determined by the City, less payments previously made.

11. EXAMINATION OF RECORDS AND AUDITS: Any authorized agent of the City, including the City Auditor or his or her representative, has the right to access, and the right to examine, copy and retain copies, at City's election in paper or electronic form, any pertinent books, documents, papers and records related to the Contractor's performance pursuant to this Agreement, provision of any goods or services to the City, and any other transactions related to this Agreement. The Contractor shall cooperate with City representatives and City representatives shall be granted access to the

foregoing documents and information during reasonable business hours and until the latter of three (3) years after the final payment under this Agreement or expiration of the applicable statute of limitations. When conducting an audit of this Agreement, the City Auditor shall be subject to government auditing standards issued by the United States Government Accountability Office by the Comptroller General of the United States, including with respect to disclosure of information acquired during the course of an audit. No examination of records and audits pursuant to this paragraph shall require the Contractor to make disclosures in violation of state or federal privacy laws. The Contractor shall at all times comply with D.R.M.C. 20-276.

12. WHEN RIGHTS AND REMEDIES NOT WAIVED: In no event shall any action by either Party hereunder constitute or be construed to be a waiver by the other Party of any breach of covenant or default which may then exist on the part of the Party alleged to be in breach, and the non-breaching Party's action or inaction when any such breach or default shall exist shall not impair or prejudice any right or remedy available to that Party with respect to such breach or default; and no assent, expressed or implied, to any breach of any one or more covenants, provisions or conditions of this Agreement shall be deemed or taken to be a waiver of any other breach.

13. OWNERSHIP, LICENSE, AND DATA.

13.1. Other than as specifically set forth in the Agreement, the Contractor does not grant or otherwise convey any license or other ownership right in or to the Works or any technology, data, or intellectual property rights associated with the Works. The Contractor grants the City a personal, limited, non-exclusive, non-transferable license (without the right to sublicense) to access and use the Works solely as contemplated by this Agreement (the "City License").

13.2. In connection with the City License, the City agrees that (a) it will not resell, assign, or otherwise transfer the Works or any portions thereof; (b) it will only use the Works for lawful purposes and will not transmit, retransmit, or store material associated with the Works in violation of any federal or state laws or regulation; (c) it will not provide access to the Works to third parties without the Contractor's knowledge; (d) it will not connect the Works to any products that the Contractor did not furnish or approve in writing; (e) it will not create derivative works based on the Works; (f) it will not disassemble, reverse engineer, decompile, or otherwise attempt to reveal the code, trade secrets, or know-how underlying the Works or allow any third party to do so; (g) it will not remove, obscure, or alter any intellectual property right or confidentiality notices or legends appearing in or on any aspect of any Works; (h) it will be responsible for distributing and assigning licenses to its end users; and (i) it will monitor and ensure that its licensed end users comply with these terms.

13.3. Unless otherwise required by law or applicable end user license terms, the City will own the recordings of communications associated with the Works (the "City Data"). During this Agreement and for a reasonable period thereafter, the Contractor will provide the City with access to the City Data.

13.4. The City grants the Contractor a limited license to use the City Data for purposes of (i) complying with the requests of officials at the Facility, (ii) disclosing information to requesting law enforcement and correctional officials as they may require for investigative, penological or

public safety purposes, (iii) performing billing and collection functions, (iv) maintaining equipment, providing the services contemplated by this Agreement and quality control purposes; (v) research and development of future services, and (vi) complying with applicable laws, regulations, or end user license terms. The City grants Contractor the exclusive right and license to install, maintain, and derive revenue from the Works at all correctional facilities under the City's authority now and in the future during the term of this Agreement. Subject to the remaining terms and conditions of this Agreement, the Contractor will be the sole and exclusive provider of incarcerated end user communications, whether fixed, mobile or otherwise, including but not limited to voice, video, and data (e.g., phone calls, video calls, messaging, prepaid calling cards, debit calling, and e-mail) and incarcerated end user software applications (e.g., automated grievance filing system, law library, etc.) at all correctional facilities now or in the future under the authority of the City and to the exclusion of any other third party providing such services, including without limitation, the City's employees, agents, or subcontractors.

- 13.5.** The deployment of certain features and functionalities within Contractor's Works which utilize third-party content or services may require a direct agreement between City and the third party as a condition which must be fulfilled prior to deployment. The City's rights to use any such third-party software product will be limited by the terms of the applicable EULA.

14. EXPRESS WARRANTIES AND DISCLAIMER

- 14.1.** For hardware and software purchased from the Contractor and owned by the City pursuant to the Agreement, the Contractor warrants that such materials will be free from material defects under normal use, maintenance, and service for a period of 90 days from the date of sale. The Contractor makes no warranty with respect to low performance, damages, or defects in any such materials caused by Breakage, nor does the Contractor make any warranty as to any such materials that the City has repaired or altered in any way. The City will be charged for reasonable repair costs incurred due to Breakage, up to the amount of the reasonable replacement costs that factor in the age and current fair market value of the specific equipment. Such charges will be deducted from the next commission payment or invoiced to the City, provided that such funds have been appropriated by the City for this Agreement. When express warranties are applicable, the Contractor will replace the applicable materials at no cost, which is the City's sole remedy in connection with a claim pursuant to this section. The Contractor warrants that the services it provides will be performed in a good and workmanlike manner consistent with industry standards and practices. The Contractor warrants that its agents and/or employees used in the performance of its obligations will be qualified to perform the contracted services. Should any errors or omissions arise in the rendering of the services under this Agreement, the Contractor will undertake to correct such errors or omissions within a reasonable time period and in compliance with the Service Level Agreement terms stated in **Exhibit C**.

- 14.2.** EXCEPT AS SPECIFICALLY SET FORTH IN THIS SECTION OR AN EXHIBIT TO THIS AGREEMENT, THE WORKS ARE PROVIDED "AS IS" AND THE CONTRACTOR DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE,

ANY IMPLIED WARRANTY ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE, AND NONINFRINGEMENT.

15. INSURANCE

- 15.1. General Conditions:** The Contractor agrees to secure, at or before the time of execution of this Agreement, the following insurance covering all operations, goods or services provided pursuant to this Agreement. The Contractor shall keep the required insurance coverage in force at all times during the term of this Agreement, including any extension thereof, and during any warranty period. The required insurance shall be underwritten by an insurer licensed or authorized to do business in Colorado and rated by A.M. Best Company as "A-VIII" or better. Each policy shall require notification to the City in the event any of the required policies be canceled or non-renewed before the expiration date thereof. Such written notice shall be sent to the parties identified in the Notices Section of this Agreement. Such notice shall reference the City contract number listed on the signature page of this Agreement. Said notice shall be sent thirty (30) days prior to such cancellation or non-renewal unless due to non-payment of premiums for which notice shall be sent ten (10) days prior. If such written notice is unavailable from the insurer, the Contractor shall provide written notice of cancellation, non-renewal and any reduction in coverage to the parties identified in the Notices Section by certified mail, return receipt requested within three (3) business days of such notice by its insurer(s) and referencing the City's contract number. The Contractor shall be responsible for the payment of any deductible or self-insured retention. The insurance coverages specified in this Agreement are the minimum requirements, and these requirements do not lessen or limit the liability of the Contractor. The Contractor shall maintain, at its own expense, any additional kinds or amounts of insurance that it may deem necessary to cover its obligations and liabilities under this Agreement.
- 15.2. Proof of Insurance:** The Contractor may not commence services or work relating to this Agreement prior to placement of coverages required under this Agreement. The Contractor certifies that the certificate of insurance attached as **Exhibit G**, preferably an ACORD form, complies with all insurance requirements of this Agreement. The City requests that the City's contract number be referenced on the certificate of insurance. The City's acceptance of a certificate of insurance or other proof of insurance that does not comply with all insurance requirements set forth in this Agreement shall not act as a waiver of the Contractor's breach of this Agreement or of any of the City's rights or remedies under this Agreement. The City's Risk Management Office may require additional proof of insurance, including but not limited to policies and endorsements.
- 15.3. Additional Insureds:** For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), the Contractor and Subcontractor's insurer(s) shall include the City and County of Denver, its elected and appointed officials, employees, and volunteers as additional insured.
- 15.4. Waiver of Subrogation:** For all coverages required under this Agreement, with the exception of Professional Liability – if required, the Contractor's insurer shall waive subrogation rights against the City.

15.5. Subcontractors and Subconsultants: The Contractor shall confirm and document that all Subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) procure and maintain coverage as approved by the Contractor and appropriate to their respective primary business risks considering the nature and scope of services provided.

15.6. Workers' Compensation and Employer's Liability Insurance: The Contractor shall maintain the coverage as required by statute for each work location and shall maintain Employer's Liability insurance with limits of \$100,000 per occurrence for each bodily injury claim, \$100,000 per occurrence for each bodily injury caused by disease claim, and \$500,000 aggregate for all bodily injuries caused by disease claims.

15.7. Commercial General Liability: The Contractor shall maintain a Commercial General Liability insurance policy with minimum limits of \$1,000,000 for each bodily injury and property damage occurrence, \$2,000,000 products and completed operations aggregate (if applicable), and \$2,000,000 policy aggregate.

15.8. Automobile Liability: The Contractor shall maintain Automobile Liability with minimum limits of \$1,000,000 combined single limit applicable to all owned, hired, and non-owned vehicles used in performing services under this Agreement.

15.9. Professional Liability (Errors & Omissions): The Contractor shall maintain minimum limits of \$1,000,000 per claim and \$1,000,000 policy aggregate limit. The policy shall be kept in force, or a Tail policy placed, for three (3) years for all contracts except construction contracts for which the policy or Tail shall be kept in place for eight (8) years.

15.10. Cyber Liability: The Contractor shall maintain Cyber Liability coverage with minimum limits of \$1,000,000 per occurrence and \$1,000,000 policy aggregate covering claims involving privacy violations, information theft, damage to or destruction of electronic information, intentional and/or unintentional release of private information, alteration of electronic information, extortion and network security. If Claims Made, the policy shall be kept in force, or a Tail policy placed, for three (3) years.

15.11. Technology Errors & Omissions: The Contractor shall maintain Technology Errors and Omissions insurance including network security, privacy liability and product failure coverage with minimum limits of \$1,000,000 per occurrence and \$1,000,000 policy aggregate. The policy shall be kept in force, or a Tail policy placed, for three (3) years.

16. DEFENSE AND INDEMNIFICATION

16.1. The Contractor hereby agrees to defend, indemnify, reimburse and hold harmless City, its appointed and elected officials, agents and employees for, from and against all liabilities, claims, judgments, suits or demands for damages to persons or property arising out of, resulting from, or relating to the Work performed under this Agreement ("Claims"), unless such Claims have been specifically determined by the trier of fact to be the sole negligence or willful misconduct of the City, its appointed and elected officials, agents, or employees. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of the Contractor or

its Subcontractors either passive or active, including City's concurrent negligence whether active or passive, except for the sole negligence or willful misconduct of City.

- 16.2.** The Contractor's duty to defend and indemnify City shall arise at the time written notice of the Claim is first provided to City regardless of whether Claimant has filed suit on the Claim. the Contractor's duty to defend and indemnify City shall arise even if City is the only party sued by claimant and/or claimant alleges that City's negligence or willful misconduct was the sole cause of claimant's damages.
- 16.3.** The Contractor will defend any and all Claims which may be brought or threatened against City and will pay on behalf of City any expenses incurred by reason of such Claims including, but not limited to, court costs and reasonable attorney fees incurred in defending and investigating such Claims or seeking to enforce this indemnity obligation. Such payments on behalf of City shall be in addition to any other legal remedies available to City and shall not be considered City's exclusive remedy.
- 16.4.** Insurance coverage requirements specified in this Agreement shall in no way lessen or limit the liability of the Contractor under the terms of this indemnification obligation. The Contractor shall obtain, at its own expense, any additional insurance that it deems necessary for the City's protection.
- 16.5.** The Contractor shall indemnify, save, and hold harmless the indemnified parties, against any and all costs, expenses, claims, damages, liabilities, and other amounts (including attorneys' fees and costs) incurred by the indemnified parties in relation to any claim that any Work provided by the Contractor under this Agreement (collectively, "IP Deliverables"), or the use thereof, infringes a patent, copyright, trademark, trade secret, or any other intellectual property right. The Contractor's obligations hereunder shall not extend to the combination of any IP Deliverables provided by the Contractor with any other product, system, or method, unless the other product, system, or method is (i) provided by the Contractor or the Contractor's subsidiaries or affiliates; (ii) specified by the Contractor to work with the IP Deliverables; (iii) reasonably required in order to use the IP Deliverables in its intended manner and the infringement could not have been avoided by substituting another reasonably available product, system, or method capable of performing the same function; or (iv) is reasonably expected to be used in combination with the IP Deliverables.
- 16.6.** The Contractor shall indemnify, save, and hold harmless the indemnified parties against all costs, expenses, claims, damages, liabilities, court awards and other amounts, including reasonable attorneys' fees and related costs, incurred by the indemnified parties in relation to the Contractor's failure to comply with §§ 24-85-101, *et seq.*, C.R.S., or the *Accessibility Standards for Individuals with a Disability* as established pursuant to § 24-85-103 (2.5), C.R.S. This indemnification obligation does not extend to the City's generated content using the Contractor's software, including any configuration or customization of the Contractor's software by the City.
- 16.7.** This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

- 17. LIMITATION OF THE CONTRACTOR'S LIABILITY:** To the extent permitted by law, the liability of the Contractor, its Subcontractors, and their respective personnel to the City for any claims, liabilities, or damages relating to this Agreement shall be limited to actual damages and unauthorized disclosure of City Data not to exceed three (3) times the Maximum Agreement Amount payable by the City under this Agreement. No limitation on the Contractor's liability to the City under this Section shall limit or affect: (i) the Contractor's indemnification obligations to the City under this Agreement; (ii) any claims, losses, or damages for which coverage is available under any insurance required under this Agreement; (iii) claims or damages arising out of bodily injury, including death, or damage to tangible property of the City; or (iv) claims or damages resulting from the recklessness, bad faith, or intentional misconduct of the Contractor or its Subcontractors.
- 18. COLORADO GOVERNMENTAL IMMUNITY ACT:** The Parties hereto understand and agree that the City is relying upon, and has not waived, the monetary limitations and all other rights, immunities and protection provided by the Colorado Governmental Act, § 24-10-101, *et seq.*, C.R.S.
- 19. CONTRACTOR COMPLIANCE WITH APPLICABLE LAWS AND POLICIES:** The Contractor shall comply with all applicable laws, rules, regulations and codes of the United States, the State of Colorado; and with the Charter, ordinances, rules, regulations, public health orders, and Executive Orders of the City and County of Denver that are applicable to the Contractor's performance hereunder. These laws, regulations, and other authorities are incorporated by reference herein to the extent that they are applicable. Any of the Contractor's personnel visiting the City's facilities will comply with all applicable City policies regarding access to, use of, and conduct within such facilities. The City will provide copies of such policies to the Contractor upon request.
- 20. CITY COMPLIANCE WITH APPLICABLE LAWS.** For Work that allow the City to monitor, record, investigate, or analyze communications, the City represents and warrants that it will operate such Work in compliance with all applicable laws, and the Contractor makes no representation or warranty as to the legality of such actions. The City may designate certain communications (for example, attorney or clergy communications) as "Private" within certain of the Work. The City acknowledges and agrees that the City has the sole discretion, authority, and responsibility to designate certain communications as Private, and that the Contractor has no discretion, authority, or responsibility to make such designations, unless done so at the City's instruction.
- 21. COMPLIANCE WITH DENVER WAGE LAWS:** To the extent applicable to the Contractor's provision of Services hereunder, the Contractor shall comply with, and agrees to be bound by, all rules, regulations, requirements, conditions, and City determinations regarding the City's Minimum Wage and Civil Wage Theft Ordinances, Sections 58-1 through 58-26 D.R.M.C., including, but not limited to, the requirement that every covered worker shall be paid all earned wages under applicable state, federal, and city law in accordance with the foregoing D.R.M.C. Sections. By executing this Agreement, the Contractor expressly acknowledges that the Contractor is aware of the requirements of the City's Minimum Wage and Civil Wage Theft Ordinances and that any failure by the Contractor, or any other individual or entity acting subject to this Agreement, to strictly comply with the foregoing D.R.M.C. Sections shall result in the penalties and other remedies authorized therein.

22. DATA PROTECTION: The Contractor recognizes and agrees that: (i) City Data is valuable property of the City; (ii) City Data may include Confidential Information, protected or regulated data, and trade secrets of the City; and (iii) the City has dedicated substantial resources to collecting, managing, protecting, and compiling City Data. The Contractor recognizes and agrees that City Data may contain personally identifiable information or other sensitive information, even if the presence of such information is not labeled or disclosed. If the Contractor receives access to City Data, the Contractor shall comply with all applicable data protection laws, including the Colorado Consumer Protection Act and the Colorado Privacy Act, to the extent applicable. Other such obligations may arise from the Health Information Portability and Accountability Act (HIPAA), IRS Publication 1075, Payment Card Industry Data Security Standard (PCI-DSS), and the FBI Criminal Justice Information Service Security Addendum. At a minimum, the Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the standards and guidelines applicable to the Contractor's performance under this Agreement. The Contractor shall also comply with the terms and conditions in the attached **Exhibit F**, Information Technology Provisions. Any Exhibit or external term hereto may not waive or modify the Contractor's legal obligations to protect City Data in compliance with applicable law under this Agreement.

23. SAFEGUARDING PERSONAL INFORMATION: "PII" means personally identifiable information including, without limitation, any information maintained by the City about an individual that can be used to distinguish or trace an individual's identity, including, but not limited to, first and last name, residence or other physical address, banking information, electronic mail address, telephone number, credit card information, an official government-issued driver's license or identification card number, social security number or tax identification number, date and place of birth, mother's maiden name, or biometric records. PII includes, but is not limited to, all information defined as personally identifiable information in §§ 24-73-101, C.R.S. "PII" shall also include "personal information" as defined in § 24-73-103(1)(g), C.R.S. If the Contractor or any of its Subcontractors receives PII under this Agreement, the Contractor shall provide for the security of such PII, in a manner and form acceptable to the City, including, without limitation, non-disclosure requirements, use of appropriate technology, security practices, computer and data access security, data storage and transmission encryption, security inspections, and audits. As applicable, the Contractor shall be a "Third-Party Service Provider" as defined in § 24-73-103(1)(i), C.R.S., and shall maintain security procedures and practices consistent with §§ 24-73-101, *et seq.*, C.R.S. In addition, as set forth in § 28-251, D.R.M.C., the Contractor, including, but not limited to, the Contractor's employees, agents, and Subcontractors, shall not collect or disseminate individually identifiable information about the national origin, immigration, or citizenship status of any person, over and above the extent to which the City is required to collect or disseminate such information in accordance with any federal, state, or local law.

24. SECURITY BREACH AND REMEDIATION

24.1. Security Breach: If the Contractor becomes aware of a suspected or unauthorized acquisition or disclosure of unencrypted data, in any form, that compromises the security, access, confidentiality, or integrity of City Data (a "Security Breach"), the Contractor shall notify the City

in the most expedient time and without unreasonable delay. A Security Breach shall also include, without limitation, (i) attempts to gain unauthorized access to a City system or City Data regardless of where such information is located; (ii) unwanted disruption or denial of service; (iii) the unauthorized use of a City system for the processing or storage of data; or (iv) changes to the City's system hardware, firmware, or software characteristics without the City's knowledge, instruction, or consent. Any oral notice of a Security Breach provided by the Contractor shall be immediately followed by a written notice to the City.

- 24.2. Remediation:** The Contractor shall implement and maintain a program for managing actual or suspected Security Breaches. In the event of a Security Breach, the Contractor shall cooperate with the City and law enforcement agencies, when applicable, to investigate and resolve the Security Breach, including, without limitation, providing reasonable assistance to the City in notifying third parties. The Contractor shall provide the City prompt access to such records related to a Security Breach as the City may reasonably request; provided such records will be the Contractor's Confidential Information, and the Contractor will not be required to provide the City with records belonging to, or compromising the security of, its other customers. The provisions of this Subsection do not limit the City's other rights or remedies, if any, resulting from a Security Breach. In addition, unless the Security Breach resulted from the City's sole act or omission, the Contractor shall promptly reimburse the City for reasonable costs incurred by the City in any investigation, remediation or litigation resulting from any Security Breach, including but not limited to providing notification to third parties whose data was compromised and to regulatory bodies, law-enforcement agencies, or other entities as required by law or contract; establishing and monitoring call center(s), and credit monitoring and/or identity restoration services to assist each person impacted by a Security Breach in such a fashion that, in the City's sole discretion, could lead to identity theft; and the payment of reasonable legal fees and expenses, audit costs, fines and penalties, and other fees imposed by regulatory agencies, courts of law, or contracting partners as a result of the Security Breach attributable to the Contractor or its Subcontractors.

25. ACCESSIBILITY AND ADA WEBSITE COMPLIANCE

- 25.1. Compliance:** The Contractor shall comply with, and the Work provided under this Agreement shall be in compliance with, all applicable provisions of §§ 24-85-101, *et seq.*, C.R.S., and the *Accessibility Standards for Individuals with a Disability*, as established pursuant to Section § 24-85-103 (2.5), C.R.S. (collectively, the "Guidelines"), to the extent required by law. The Contractor shall also comply with Level AA of the most current version of the Web Content Accessibility Guidelines (WCAG), incorporated in the State of Colorado technology standards.
- 25.2. Testing:** The City may require the Contractor's compliance to be determined by a third party selected by the City to attest that the Contractor's has performed all obligations under this Agreement in compliance with §§ 24-85-101, *et seq.*, C.R.S., and the Accessibility Standards for Individuals with a Disability as established pursuant to § 24-85-103 (2.5), C.R.S.
- 25.3. Validation and Remediation:** The Contractor agrees to promptly respond to and resolve any instance of noncompliance regarding accessibility in a timely manner and shall remedy any noncompliant Work at no additional cost to the City. If the City reasonably determines

accessibility issues exist, the Contractor shall provide a “roadmap” for remedying those deficiencies on a reasonable timeline to be approved by the City. Resolution of reported accessibility issue(s) that may arise shall be addressed as high priority, and failure to make satisfactory progress towards compliance with the Guidelines, as agreed to in the roadmap, shall constitute a breach of contract and be grounds for termination or non-renewal of this Agreement.

26. CONFIDENTIAL INFORMATION

- 26.1.** “Confidential Information” means all information or data, regardless of form, not subject to disclosure under the Colorado Open Records Act, §§ 24-72-201, *et seq.*, C.R.S. (“CORA”), and is marked or identified at the time of disclosure as being confidential, proprietary, or its equivalent. Each of the Parties may disclose (a “Disclosing Party”) or permit the other Party (the “Receiving Party”) access to the Disclosing Party’s Confidential Information in accordance with the following terms. Except as specifically permitted in this Agreement or with the prior express written permission of the Disclosing Party, the Receiving Party shall not: (i) disclose, allow access to, transmit, transfer or otherwise make available any Confidential Information of the Disclosing Party to any third party other than its employees, Subcontractors, agents and consultants that need to know such information to fulfill the purposes of this Agreement, and in the case of non-employees, with whom it has executed a non-disclosure or other agreement which limits the use, reproduction and disclosure of the Confidential Information on terms that afford at least as much protection to the Confidential Information as the provisions of this Agreement; or (ii) use or reproduce the Confidential Information of the Disclosing Party for any reason other than as reasonably necessary to fulfill the purposes of this Agreement. This Agreement does not transfer ownership of Confidential Information or grant a license thereto. The Parties will retain all right, title, and interest in its Confidential Information.
- 26.2.** The Contractor shall provide for the security of Confidential Information and information which may not be marked but constitutes personally identifiable information or other federally or state regulated information (“Regulated Data”) in accordance with all applicable laws and regulations. If the Contractor receives Regulated Data outside the scope of this Agreement, it shall promptly notify the City.
- 26.3.** Disclosed information or data that the Receiving Party can establish: (i) was lawfully in the Receiving Party’s possession before receipt from the Disclosing Party; or (ii) is or becomes a matter of public knowledge through no fault of the Receiving Party; or (iii) was independently developed or discovered by the Receiving Party; or (iv) was received from a third party that was not under an obligation of confidentiality, shall not be considered Confidential Information under this Agreement. The Receiving Party will inform necessary employees, officials, Subcontractors, agents, and officers of the confidentiality obligations under this Agreement, and all requirements and obligations of the Receiving Party under this Agreement shall survive the expiration or earlier termination of this Agreement.
- 26.4.** Nothing in this Agreement shall in any way limit the ability of the City to comply with any laws or legal process concerning disclosures by public entities. The Parties understand that all materials exchanged under this Agreement, including Confidential Information, may be subject

to CORA. In the event of a request to the City for disclosure of possible confidential materials, the City shall promptly notify the Contractor of such request to give the Contractor the opportunity to object to the disclosure of any of its materials which it marked as, or otherwise asserts is, proprietary or confidential. If the Contractor objects to disclosure of any of its material, the Contractor shall identify to the City the legal basis under CORA for any right to withhold. In the event of any action or the filing of a lawsuit to compel disclosure, the Contractor agrees to intervene in such action or lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. If the matter is not resolved, the City will tender all material to the court for judicial determination of the issue of disclosure. The Contractor further agrees to defend, indemnify, and save and hold harmless the City, its officers, agents, and employees, from any claim, damages, expense, reasonable attorneys' fees, or costs arising out of the Contractor's intervention to protect and assert its claim of privilege against disclosure under this Section.

27. PROTECTED HEALTH INFORMATION: When applicable, the Contractor shall comply with all legislative and regulatory requirements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA"); the Health Information Technology for Economic and Clinical Health Act ("HITECH"); 42 CFR Part 2, Confidentiality of Substance use Disorder Patient Records; the privacy standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160 and 164, Subparts A and E; and the security standards adopted by the U.S. Department of Health and Human Services, 45 C.F.R. Parts 160, 162, 164, and Subpart C (collectively, "HIPAA Rules"). The Contractor shall implement all necessary protective measures to comply with HIPAA Rules, and the Contractor hereby agrees to be bound by the terms of the Business Associate Agreement attached hereto and incorporated herein as **Exhibit D**. The Contractor shall not use protected health information or substance use treatment records except as legally necessary to fulfill the purpose of this Agreement and shall hold the City harmless, to the extent permitted by law, for any breach of these regulations. This Section shall survive the expiration or earlier termination of this Agreement, and the Contractor shall ensure that the requirements of this Section are included in any relevant subcontracts or subgrants.

28. CRIMINAL JUSTICE INFORMATION: The Contractor shall comply with all applicable standards of the Criminal Justice Information Services ("CJIS") Security Policy, attached hereto and incorporated herein as **Exhibit E** and all other requirements issued by the Federal Bureau of Investigation ("FBI"). The Contractor shall ensure that any Work provided under this Agreement protects the confidentiality, integrity, and availability of criminal justice information ("CJI") from unauthorized access, use, or disclosure. The Contractor shall ensure its responsibilities related to CJIS compliance are appropriately assigned and maintained and shall cooperate with any audits or inspections conducted by the City, the Colorado Bureau of Investigations, or the FBI to verify compliance with the CJIS Security Policy. The Contractor shall promptly report any breaches or incidents involving CJI to the City and take appropriate remedial actions. Contractors with direct access or indirect access to CJI shall handle all CJI following the CJIS Security Policy and Title 28, Code of Federal Regulations, Part 20 (relevant standards). Contractors supporting systems which provide direct access to CJI shall also follow the regulations listed in the laws, policies, and manuals

incorporated into this agreement: NCIC Operating Manual, CCIC Training Manual, Interstate Identification Index / National Fingerprint File Operational and Technical Manual, and Title 28, Code of Federal Regulations, Part 23. Contractors who perform criminal justice functions and have access to CJI shall meet the same training and certification criteria required of governmental agencies performing a similar function and are subject to audit to the same extent as local agencies. Before receiving access to CJI or Federal Criminal History Record Information (“CHRI”), the Contractor and its individual employees must complete the attached CJIS Security Addendum certification attached hereto. The Contractor shall maintain signed CJIS Security Addendum certification pages for its personnel and shall provide copies to the City upon request.

- 29. ASSIGNMENT; SUBCONTRACTING:** The Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the City’s prior written consent, which cannot be unreasonably withheld. Any assignment or subcontracting without such consent will be ineffective and void and shall be cause for termination of this Agreement by the City. The City has sole and absolute discretion whether to consent to any assignment or subcontracting, or to terminate this Agreement because of unauthorized assignment or subcontracting. The City, at their reasonable discretion, may approve of the assignment or transfer in writing, deny the assignment or transfer, or refer the matter to the City’s governing bodies for approval. In the event of any subcontracting or unauthorized assignment: (i) the Contractor shall remain responsible to the City; and (ii) no contractual relationship shall be created between the City and any subconsultant, Subcontractor, or assign.
- 30. NO THIRD-PARTY BENEFICIARY:** Enforcement of the terms of this Agreement and all rights of action relating to enforcement are strictly reserved to the Parties. Nothing contained in this Agreement gives or allows any claim or right of action to any third person or entity. Any person or entity other than the City or the Contractor receiving services or benefits pursuant to this Agreement is an incidental beneficiary only.
- 31. NO AUTHORITY TO BIND CITY TO CONTRACTS:** The Contractor lacks any authority to bind the City on any contractual matters. Final approval of all contractual matters that purport to obligate the City must be executed by the City in accordance with the City’s Charter and the Denver Revised Municipal Code.
- 32. AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS:** Except for the functional requirements provided in response to a request for proposal and/or any subsequent enhancement of the SOW or other implementation documentation that may be developed after execution of this Agreement, this Agreement is the complete integration of all understandings between the Parties as to the subject matter of this Agreement. No prior, contemporaneous, or subsequent addition, deletion, or other modification has any force or effect, unless embodied in this Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of this Agreement or any written amendment to this Agreement will have any force or effect or bind the City.
- 33. SEVERABILITY:** Except for the provisions of this Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision

of this Agreement or any portion of it to be invalid, illegal, or unenforceable, the validity of the remaining portions or provisions will not be affected, if the intent of the Parties can be fulfilled.

- 34. CONFLICT OF INTEREST:** No employee of the City shall have any personal or beneficial interest in the Services or property described in this Agreement. The Contractor shall not hire, or contract for services with, any employee or officer of the City that would be in violation of the City's Code of Ethics, D.R.M.C. § 2-51, *et seq.* or the Charter §§ 1.2.8, 1.2.9, and 1.2.12. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under this Agreement. The Contractor represents that it has disclosed any and all current or potential conflicts of interest. A conflict of interest shall include transactions, activities or conduct that would affect the judgment, actions or work of the Contractor by placing the Contractor's own interests, or the interests of any party with whom the Contractor has a contractual arrangement, in conflict with those of the City. The City, in its sole discretion, will determine the existence of a conflict of interest and may terminate this Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.
- 35. NOTICES:** All notices required by the terms of this Agreement must be hand delivered, sent by overnight courier service, mailed by certified mail, return receipt requested, or mailed via United States mail, postage prepaid, if to the Contractor at the aforementioned address, and if to the City at: Denver Department of Safety, 1331 Cherokee Street, Room 302, Denver, Colorado 80204; with copies to: Denver City Attorney's Office, 1437 Bannock St., Room 353, Denver, Colorado 80202; and Chief Information Officer, Denver Technology Services, 201 West Colfax Avenue, Dept. 301, Denver, Colorado 80202. Unless otherwise provided in this Agreement, notices shall be effective upon delivery of the written notice. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. If a Party delivers a notice through email and the email is undeliverable, then, unless the Party has been provided with an alternate email contact, the Party delivering the notice shall deliver the notice by certified or registered mail to the addresses set forth herein. The Parties may designate electronic and substitute addresses where or persons to whom notices are to be mailed or delivered. However, these substitutions will not become effective until actual receipt of written notification.
- 36. DISPUTES:** All disputes between the City and the Contractor arising out of or regarding this Agreement will be resolved by administrative hearing pursuant to the procedure established by D.R.M.C. § 56-106(b)-(f). For the purposes of that administrative procedure, the City official rendering a final determination shall be the CIO as defined in this Agreement. In the event of a dispute between the Parties, the Contractor will continue to perform its obligations under this Agreement during the resolution of the dispute until this Agreement is terminated in accordance with its terms.
- 37. GOVERNING LAW; VENUE:** This Agreement will be construed and enforced in accordance with applicable federal law, the laws of the State of Colorado, and the Charter, Revised Municipal Code, ordinances, regulations and Executive Orders of the City and County of Denver, which are expressly incorporated into this Agreement. Unless otherwise specified, any reference to statutes, laws, regulations, charter or code provisions, ordinances, executive orders, or related memoranda, includes

amendments or supplements to same. Venue for any legal action relating to this Agreement will be in the District Court of the State of Colorado, Second Judicial District (Denver District Court).

- 38. NO DISCRIMINATION IN EMPLOYMENT:** In connection with the performance of work under this Agreement, the Contractor may not refuse to hire, discharge, promote, demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, ethnicity, citizenship, immigration status, gender, age, sexual orientation, gender identity, gender expression, marital status, source of income, military status, protective hairstyle, or disability. The Contractor shall insert the foregoing provision in all subcontracts.
- 39. LEGAL AUTHORITY:** The Contractor represents and warrants that it possesses the legal authority, pursuant to any proper, appropriate, and official motion, resolution or action passed or taken, to enter into this Agreement. Each person signing and executing this Agreement on behalf of the Contractor represents and warrants that he has been fully authorized by the Contractor to execute this Agreement on behalf of the Contractor and to validly and legally bind the Contractor to all the terms, performances and provisions of this Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate this Agreement if there is a dispute as to the legal authority of either the Contractor or the person signing this Agreement to enter into this Agreement.
- 40. LITIGATION REPORTING:** If the Contractor is served with a pleading or other document in connection with an action before a court or other administrative decision making body, and such pleading or document relates to this Agreement or may affect the Contractor's ability to perform its obligations under this Agreement, the Contractor shall, within 10 days after being served, notify the City of such action and deliver copies of such pleading or document, unless protected by law, to the City.
- 41. LICENSES, PERMITS, AND OTHER AUTHORIZATIONS:** The Contractor shall secure, prior to the Term, and shall maintain, at its sole expense, all licenses, certifications, rights, permits, and other authorizations required to perform its obligations under this Agreement. This Section is a material part of this Agreement.
- 42. NO CONSTRUCTION AGAINST DRAFTING PARTY:** The Parties and their respective counsel have had the opportunity to review this Agreement, and this Agreement will not be construed against any party merely because any provisions of this Agreement were prepared by a particular party.
- 43. ORDER OF PRECEDENCE:** In the event of any conflicts between the provisions in the body of this Agreement, the Exhibits, or any other attachment hereto, the provisions in the body of this Agreement shall control. For the avoidance of doubt, no terms within any subsequent order form, invoice, or quote issued by the Contractor to the City shall be binding on the City or take precedence over the terms of the body of this Agreement regardless of any term contained therein to the contrary.
- 44. SURVIVAL OF CERTAIN PROVISIONS:** The terms of this Agreement and any Exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of this Agreement survive this Agreement and will continue to be enforceable. Without limiting the generality of this provision, the Contractor's obligations to provide insurance and to indemnify the City will survive for a period equal to any and all relevant statutes of limitation, plus the time necessary to fully resolve any claims, matters, or actions begun within that

period. Furthermore, a grant of property or intellectual property rights to the City that by its terms continues for longer than the duration of this Agreement will survive expiration or termination of this Agreement, except termination for the City's breach of its obligations to pay for such property or rights. Promptly after termination or expiration of this Agreement, in whole or in part, either Party shall promptly return to the other Party all its Data and all other information provided by the requesting Party in such format as the requesting Party may reasonably require and permanently erase all copies thereof.

- 45. INUREMENT:** The rights and obligations of the Parties herein set forth shall inure to the benefit of and be binding upon the Parties hereto and their respective successors and assigns permitted under this Agreement.
- 46. TIME IS OF THE ESSENCE:** The Parties agree that in the performance of the terms, conditions, and requirements of this Agreement, time is of the essence.
- 47. FORCE MAJEURE:** Neither Party shall be responsible for failure to fulfill its obligations hereunder or liable for damages resulting from delay in performance as a result of war, fire, strike, riot or insurrection, natural disaster, unreasonable delay of carriers, governmental order or regulation, complete or partial shutdown of manufactures, unreasonable unavailability of equipment or software from suppliers, default of a Subcontractor or vendor (if such default arises out of causes beyond their reasonable control), the actions or omissions of the other Party and/or other substantially similar occurrences beyond the Party's reasonable control ("Excusable Delay"). In the event of any such Excusable Delay, time for performance shall be extended for as may be reasonably necessary to compensate for such delay.
- 48. UNCONTROLLABLE CIRCUMSTANCES:** The financial arrangements in this Agreement are based on conditions existing as of the Effective Date; including, without limitation, any representations regarding existing and future conditions made by the City in connection with the negotiation and execution of this Agreement. If conditions change due to causes beyond the Contractor's control (including, but not limited to, a change in the scope of Contractor's services; changes in rates, regulations, or operations mandated by law; material reduction in facility population or capacity; material changes in jail policy; material change in economic conditions; actions the City takes for security reasons (e.g., lockdowns); or acts of God) which would negatively impact the Contractor's business, the Parties agree to negotiate in good faith a modification to the Agreement to offset the impact of such change; however, nothing herein shall obligate the City to issue any amendment to this Agreement. The foregoing shall be in addition to, and without limitation of, the Parties' rights and obligations set forth herein in respect of an event of Force Majeure or any other rights of Contractor to adjust pricing set forth in this Agreement. Further, City acknowledges that Contractor's provision of the services is subject to certain federal, state, or local regulatory requirements and restrictions that are subject to change from time-to-time and that Contractor may take any steps necessary to perform in compliance therewith.
- 49. COMPLIANCE WITH FCC REGULATIONS:** In July 2024, the Federal Communications Commission issued its final regulations implementing the Martha-Wright Reed Act (the "2024 FCC Order"). The Parties acknowledge that the 2024 Order's requirements impact, among other things, maximum calling rates, the charging of ancillary and other fees, commissions that can be paid to

agencies, the types of allowable reimbursement payments that can be made to agencies, and the types of in-kind services providers may not offer to agencies. This Agreement includes terms to comply with the 2024 FCC Order. The Parties agree that, if and when the 2024 Order is overturned or otherwise is no longer in effect in whole or part, the Parties will negotiate the terms of this Agreement to the extent possible to address such change, or the Agreement will be modified automatically as of the relevant date as necessary and without the need for a written modification of this Agreement to comply with such change.

50. **PARAGRAPH HEADINGS**: The captions and headings set forth herein are for convenience of reference only and shall not be construed to define or limit the terms and provisions hereof.
51. **CITY EXECUTION OF AGREEMENT**: This Agreement is expressly subject to and shall not be or become effective or binding on the City until it has been fully executed by all signatories of the City and County of Denver.
52. **ADVERTISING AND PUBLIC DISCLOSURE**: The Contractor shall not include any reference to this Agreement or to Services performed pursuant to this Agreement in any of the Contractor's advertising or public relations materials without first obtaining the City's written approval. Any oral presentation or written materials related to Services performed under this Agreement will be limited to Services that have been accepted by the City. The Contractor shall notify the City in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.
53. **EXTERNAL TERMS AND CONDITIONS DISCLAIMER**: Notwithstanding anything to the contrary herein, the City shall not be subject to any provision including any terms, conditions, or agreements, and links thereto, appearing on the Contractor's or a Subcontractor's website, forms, or any provision incorporated into any click-through or online agreements related to the Work unless that provision is specifically incorporated into this Agreement.
54. **PROHIBITED TERMS**: Any term included in this Agreement that requires the City to indemnify or hold the Contractor harmless; requires the City to agree to binding arbitration; limits the Contractor's liability for damages resulting from death, bodily injury, or damage to tangible property; requires payment for any obligation where there has not been an appropriation; requires venue and jurisdiction outside of the Colorado; or seeks to modify the order of precedence, as stated in the main body of this Agreement; or that conflicts with this provision in any way shall be *void ab initio*. All contracts entered into by the City, except for certain intergovernmental agreements, shall be governed by Colorado law notwithstanding any term or condition to the contrary.
55. **USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS**: To the extent applicable, the Contractor shall cooperate and comply with the provisions of Executive Order 94 and Attachment A thereto concerning the use, possession or sale of alcohol or drugs. Violation of these provisions or refusal to cooperate with implementation of the policy can result in the City barring the Contractor from City facilities or participating in City operations.
56. **COUNTERPARTS OF THIS AGREEMENT**: This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

57. ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS: The Contractor consents to the use of electronic signatures by the City. This Agreement, and any other documents requiring a signature hereunder, may be signed electronically by the City in the manner specified by the City. The Parties agree not to deny the legal effect or enforceability of this Agreement solely because it is in electronic form or because an electronic record was used in its formation. The Parties agree not to object to the admissibility of this Agreement in the form of an electronic record, or a paper copy of an electronic document, or a paper copy of a document bearing an electronic signature, on the ground that it is an electronic record or electronic signature or that it is not in its original form or is not an original.

58. ATTACHED EXHIBITS INCORPORATED: The following attached exhibits are hereby incorporated into and made a material part of this Agreement: **Exhibit A**, Scope of Work; **Exhibit B**, End-of-Contract Extraction; **Exhibit C**, Service Level Agreement; **Exhibit D**, HIPAA/HITECH BAA; **Exhibit E**, Criminal Justice Information Services Security Addendum; **Exhibit F**, Information Technology Provisions; and **Exhibit G**, Certificate of Insurance.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



Contract Control Number:
Contractor Name:

TECHS-202577792-00
SECURUS TECHNOLOGIES LLC

IN WITNESS WHEREOF, the parties have set their hands and affixed their seals at
Denver, Colorado as of:

SEAL**CITY AND COUNTY OF DENVER:**

ATTEST:

By: _____

APPROVED AS TO FORM:

Attorney for the City and County of Denver

By: _____

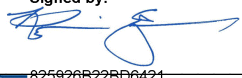

REGISTERED AND COUNTERSIGNED:

By: _____

By: _____

Contract Control Number:
Contractor Name:

TECHS-202577792-00
SECURUS TECHNOLOGIES LLC

Signed by:

By:  825926B22BD6421...

Name: Kevin Elder
(please print)

Title: President
(please print)

ATTEST: [if required]

By: _____

Name: _____
(please print)

Title: _____
(please print)

Exhibit A – Scope of Work

The City and County of Denver’s Department of Safety Detention (DSD) seeks a comprehensive telephone and video visitation solution for its detention facilities. The aim is to ensure safe, secure, and equitable communication services for individuals in custody while supporting operational efficiency and the community’s needs.

The scope of services includes:

1. **Hardware Provisioning:**
 - Telephones, kiosks, tablets, servers, switches, and all necessary Wi-Fi infrastructure.
 - Internet connection provided by Contractor.
2. **Software Solutions:**
 - Video and telephone visitation platforms.
 - Fraud prevention through Contractor’s voice biometrics investigative tools.
 - Digital mail solutions.
 - Integration with Jail Management System (JMS) and commissary systems.
3. **Educational and Career Resources:**
 - Access to materials that foster personal growth and professional development.
4. **Reporting and Analytics:**
 - Business intelligence capabilities for operational insights.
5. **System Maintenance and Upgrades:**
 - Consistent updates of software, hardware, and firmware to maintain modern standards.
 - Replacement of end-of-life equipment at no cost to the City.
6. **Security and Compliance:**
 - Configurable access and security settings to meet operational and legal standards.

Facilities Overview

1. **Downtown Detention Center (DDC):**
 - Average population: 1,148 individuals.
 - Infrastructure: 119 kiosks, 2 mobile kiosks, 43 wall phones.
2. **County Jail (COJL):**
 - Average population: 565 individuals.
 - Infrastructure: 49 kiosks, 65 phones.

Cost and Compensation

Any fixed amount described in this Scope of Work to be paid by the City will be invoiced by the Contractor. Invoices are due and payable 30 days from invoice date. All commissions to be paid by the Contractor to the City will be remitted monthly, within 30 days after the close of each calendar month. Payments are final unless written objections are submitted within 60 days of the Payment Date.

Requirements

Installation and Cutover

1. **Implementation Plan:**
 - Submission of a detailed schedule covering installation, utility coordination, training, testing, and cutover activities.
 - Minimized disruption to facility operations during installation.
2. **Vendor Responsibilities:**
 - Full assumption of risks for equipment shipment, unloading, and installation.
 - Adherence to quality standards using Securus' five-phase implementation plan with Six Sigma quality controls.

Post-Implementation Support

1. **24/7 Support:**
 - Dedicated Account and Field Services Managers.
 - Toll-free technical support available 24/7/365.
2. **Training:**
 - Initial and ongoing training for facility staff to maximize system utilization.
 - Training methods: hands-on sessions, online courses, and refresher training programs.
3. **Performance Reviews:**
 - Quarterly operational reviews with the City and County team.
 - Monitoring of key performance metrics, system usage, and service reliability.

Technology and Equipment

1. **Upgrades and Maintenance:**
 - Consistent replacement of outdated or unsupported equipment at no cost.
 - Immediate action on end-of-life components.
2. **Integration and Compatibility:**
 - Full compatibility with existing City systems (JMS, commissary, etc.).

Minimizing Transition Impact

- Comprehensive transition plan to mitigate disruptions for incarcerated individuals, their families, and facility staff.
 - Pre-transition outreach and communication to inform stakeholders about system changes and usage.
 - Minimization of service downtime through strategic planning and execution.
-

Deliverables

1. Turnkey installation of all equipment and connectivity.
2. Robust fraud prevention, security, and analytics tools.
3. Comprehensive training and support for facility staff.
4. Quarterly reviews and reports tailored to City needs.
5. Continuous system enhancements and equipment updates throughout the contract term.

This document establishes the foundation for collaboration between the City of Denver and Securus Technologies, requiring high-quality service delivery and operational excellence.

Implementation Phases and Methodology

Securus Technologies will employ a structured **five-phase implementation plan**, designed to ensure seamless deployment and transition. Quality control checkpoints will be integrated throughout to meet or exceed City and County specifications.

Phase 1: Project Initiation

- **Kick-Off Meeting:** Onsite introductions, scope review, and project timelines.
- **Site Survey Confirmation:** Verification of facility requirements and system needs.
- **Communication Plan:** Establishment of channels for updates and feedback throughout the project.

Phase 2: Project Planning

- Coordination of materials, human resources, and logistics.
- Scheduling of equipment deliveries and site access.
- Network service and equipment installation coordination with interstate and local carriers.

Phase 3: Project Execution

- **Pre-Installation Activities:** Wiring, hardware staging, and initial testing.
- **System Installation:** Deployment of kiosks, phones, and video visitation units.
- **Testing and Walk-Through:** Initial system validation and review with facility staff.
- **Staff Training:** Onsite and virtual sessions to ensure immediate usability post-installation.

Phase 4: Monitoring and Controlling

- Resolution of outstanding issues.
- Daily diagnostic checks to confirm system performance.
- Quality control checkpoint: Functional validation of system capabilities.

Phase 5: Project Closure

- Final project review and acceptance by City and County stakeholders.
 - Handover of ongoing maintenance and support responsibilities to the dedicated Securus Account Manager.
 - Delivery of relevant project documentation, including network schematic diagrams and equipment inventories.
-

Support and Maintenance

24/7 Technical Support

- Access to a team of technical specialists through a toll-free line or email.
- Escalation procedures provided to ensure rapid response for critical issues.

Quarterly Performance Reviews

- Regular evaluations of service delivery, including system uptime, operational challenges, and potential upgrades.
- Collaborative identification of improvement opportunities.

Proactive Maintenance

- Continuous monitoring to identify and address equipment or software issues before they impact operations.
 - Replacement of end-of-life systems with new, compatible technology at no cost.
-

Additional Considerations

Minimizing Transition Impact

- **Stakeholder Communication:**
 - A pre-launch campaign to inform families and other stakeholders of the new system, its features, and how to use it.
 - Provision of detailed guides, including web and phone support details.
- **Downtime Mitigation:**
 - Strategic scheduling to limit service interruptions.
 - Activities such as system testing or cut over executed during regular business hours, to be priorly agreed to between the parties.

Compliance and Reporting

- Systems will be configured to meet local, state, and federal regulations.

- Customizable reporting tools to provide real-time insights into system usage, call volumes, and other key metrics.

Scalability and Future Growth

- The system will be scalable to support potential facility expansions or additional service needs.
- Vendor will proactively introduce new technologies to align with industry advancements.

Key Performance Indicators (KPIs)

To ensure accountability and service excellence, the following KPIs will be monitored and reported:

1. **System Uptime:** Target of 99% availability.
2. **Service Response Time:** Maximum 2-hour response for critical issues.
3. **Installation Milestones:** Adherence to the agreed project timeline.
4. **User Training Completion:** All staff trained and proficient within two weeks of installation.
5. **Quarterly Review Compliance:** Timely submission and discussion of performance reviews.

Seamless System Integration and Maintenance

As the incumbent provider, Securus has already deployed and operationalized the necessary equipment, including video visitation units, server racks, software, and uninterrupted power supplies. These systems are fully functional and seamlessly integrated with the City and County's processes, ensuring:

- **No transition downtime** or risks to system performance.
- A robust operational framework that eliminates the need for cutovers or disruptions.

Securus shall continuously delivers **NextGen SCP software upgrades and system updates** three to four times annually, ensuring the system evolves alongside technological advancements and industry demands. These updates provide:

- New features and functionalities to address evolving operational and security challenges.
- Zero downtime during deployment, maintaining uninterrupted service.

Equipment Lifecycle Management

Securus shall ensure sustained operational excellence through:

- Replacement of end-of-life equipment on an **as-needed basis at no additional cost**.
- Regular testing and validation to guarantee high traffic performance and proper system operation.

Quality Assurance and Customer-Centric Feedback

Securus shall employ an extensive quality management framework to enhance system reliability and customer satisfaction. This includes:

1. **Transactional Surveys**
 - Feedback gathered post-installation, changes, repairs, and other key events.
 - Any low ratings (1 or 2 out of 5) trigger immediate management review and corrective action.
 2. **Relationship Surveys**
 - Periodic evaluations of customer expectations and service performance.
 - A structured improvement plan is implemented for low ratings.
 3. **User Groups**
 - Opportunities for customers to share ideas and address operational challenges, influencing future product development and innovation.
-

Advanced System and Platform Design

Securus shall employ a formalized **Software Development Lifecycle (SDLC)** for feature enhancements, focusing on rigorous testing and seamless functionality. Each phase—Analysis, Design, Development, Quality Assurance, Implementation, and Post-Implementation Support—ensures:

- High-quality deliverables with minimal rework.
- System stability across distinct environments: Development, Quality Assurance, Pre-Production, and Production.

Quality assurance tests include:

- **Load Testing:** Validates system response under high traffic.
 - **Performance and Regression Testing:** Ensures user experience and compatibility of new features.
 - **Exception Testing:** Tests resilience against unexpected scenarios.
-

Installation and Quality Control

Securus shall emphasize precision and excellence during installation through structured quality control checkpoints:

1. **Provisioning Review:** Verification by engineers, project managers, and account managers.
2. **Pre-Installation Checklist:** Field technicians ensure physical standards are met.

3. **Equipment Testing:** Includes functional validation and test scenarios for call configurations.
4. **Acceptance Review:** Comprehensive review with documentation provided to the City and County for final approval.

Telephone Service / Call Management System

Secure Call Platform: Secure Call Platform (“SCP”) allows end users to place calls through its centralized system without the need for conventional live operator services. SCP allows customers to (a) monitor and record calls; (b) prevent monitoring and recording of private calls; (c) limit the duration of calls; (d) maintain call detail records; (e) shut the System on or off; and (f) allow free calls. Contractor will be responsible for all billing and collections of calling charges but may contract with third parties to perform such function.

Contractor will provide the equipment needed to support the required number and type of phones and other components in connection with SCP. Additional equipment or applications will be installed only upon mutual agreement by the parties and may incur additional charges.

Contractor will charge \$0.06 per minute for all calls placed to and from incarcerated end users within the Facility, plus applicable taxes and regulatory or other government-imposed fees. International rates may vary from country to country. Contractor will also provide 2 calls per week for each incarcerated end user at no cost to the incarcerated end user. No cost calls do not carry over to the following weeks and are non-transferable between incarcerated end users.

Securus Debit. The Securus Debit Account is a prepaid account where Contractor holds the incarcerated individual’s funds authorized to use for Contractor services. Deposits to this account originate through both incarcerated individual transfer of funds from their commissary at the facility or externally by family and friends direct contribution into the account.

When an incarcerated individual initiates the authorization for a funds transfer from the commissary through Contractor’s phone system, those funds are immediately available for use on Securus Debit Account. However, the actual movement of the money does not happen until Contractor invoices the City for that purchase of prepaid Contractor services and the City pays that invoice. Invoices are due and payable upon receipt.

Actual incarcerated individual consumption of Contractor services (phone usage, tablet content, etc.) causes a reduction in the Securus Debit Account balance on the Securus accounting books until the balance is used or refunded to the incarcerated individual. Note that this is not a “bank account” as the incarcerated individual is pre-paying for future communications services from Contractor. This account is managed by Contractor accounting as a Contractor obligation for providing the service from the prepaid funds already transferred. Any balance in the Securus Debit Account will be refunded directly to the incarcerated individual or facility for distribution upon release.

SCP also includes the ability to integrate Securus Debit accounts. Securus Debit accounts are associated with a personal identification number (“PIN”), and users are required to input a PIN at the beginning of

every Securus Debit call.

Commissary Order by Phone

Through Commissary Order by Phone, incarcerated end users may order and purchase commissary items using the phone system. The City's commissary operator provides an interactive voice response system ("IVR") and a speed-dial number (800#) into the commissary's IVR. Contractor will work with the City's commissary provider to set up and activate Commissary Order by Phone at the Facility.

Securus Video Connect / Connectus

Securus Video Connect ("SVC") is a web-based video conference system. SVC runs on the ConnectUs Service Platform ("ConnectUs"), a communications and services platform that allows for the consolidation of assorted activities in a single interface with a customized mix of applications ("ConnectUs Applications"). **CONNECTUS APPLICATIONS:** Contractor will deploy its Video Connect, Phone Call, Forms (Grievance), Handbook (.PDF), Third Party Vendor Commissary, Edovo Education Suite, Website Education (URL), Videos (.MP4), Self-Op Commissary Ordering, Emergency Visitation, Job Search, and FastCase, Law Library ConnectUs Applications at no additional cost.

Additional Connectus Applications may be deployed by mutual agreement of Contractor and the City. If applicable, Contractor will deploy a connector to a Third Party Vendor Commissary Application, once an agreement has been executed by and between Contractor and the City's commissary operator for such application. Contractor will not charge an integration fee, but the City is responsible for any Jail Management System (JMS) and Commissary integration fees if charged by those providers.

The City also agrees to implement the following additional requirements:

1. The City agrees that SVC must be available for paid remote sessions seven days a week for a minimum of 80 hours per terminal per week.
2. The City will allow incarcerated end users to conduct remote visits without quantity limits other than for disciplinary action for individual misbehavior.
3. All on-site sessions will be required to be scheduled at least 24 hours in advance, where practicable.

Contractor will offer 1 SVC 10-minute session per week per incarcerated end user at no cost to the incarcerated end user until Contractor can charge for SVC minutes in compliance with the 2024 FCC Order. Contractor will communicate to the City when Contractor will resume charging for SVC minutes, the cost to the incarcerated end user, and any other terms and conditions to SVC if applicable. In addition to SVC calls charged by the minute, Contractor will continue to provide 1 SVC call per incarcerated end user per week at no cost to the City or the incarcerated end user. No cost SVC calls are non-transferable and noncumulative.

Video Relay Service

Contractor's Video Relay Service application ("VRS") provides a fully integrated video relay service offering into the Secure Call Platform (SCP) allowing critical call controls to be maintained. This service allows deaf and hard-of-hearing incarcerated end users the ability to communicate with friends and family via a videoconferencing service.

The City is solely responsible for (a) determining which individuals are eligible to use VRS; (b) configuring SCP to allow access to the VRS application on ConnectUs-enabled terminals; and (c) designating which VRS numbers for which calls are not to be recorded, by marking those numbers as "private" within SCP. Contractor's third-party vendors shall have the right, in their discretion, to terminate VRS sessions for policy violations or disruptive behavior, including, without limitation, verbal or other abuse of the VRS interpreter.

Contractor will provide the VRS at no cost to the City.

Tablet

The Securus Unity Tablet Program shall offer a robust, corrections-grade solution tailored to the unique needs of Denver Sheriff facilities, ensuring secure, efficient, and user-friendly technology for incarcerated individuals. The program shall include:

Tablet Services Overview

- **Device Overview:**
 - **Screen Type:** Touch-screen interface requiring no prior training or device experience.
 - **Device Size:** Compact, durable, and ergonomically designed for individual use.
 - **Operating System:** Custom-developed proprietary firmware, hardened to eliminate unauthorized access.
 - **Battery Specifications and Charging Options:**
 - **Personal Wired Charging:** Tablets can be charged using barrel cable chargers, typically incompatible with non-Securus devices to prevent contraband usage.
 - **Community Wired Charging Stations:** Configurations include 16, 40, or 80-count wall-mounted stations or rolling carts.
 - Offline charging allows uninterrupted content consumption during charging.
- **Preloaded Content:** Corrections-appropriate applications, communication tools, and educational resources updated automatically via secure Wi-Fi connections.
- **Content Customization:** Facilities shall be able to control applications, access permissions, and schedules through Command & Control Officer Tablets.

Security Features

1. **Tablet Firmware Security:**

- Removal of consumer-grade features like browser, contacts, calendar, messaging clients, and third-party app stores.
- Disabling of NFC and Bluetooth (except for approved Wi-Fi).
- Apps are authorized and managed exclusively by Securus, preventing installation or deletion by users.

2. **Wi-Fi Access and Restrictions:**

- Tablets connect only to Securus-provided networks with a unique SSID, blocking all public internet access.
- Custom wireless access points (WAPs) ensure exclusive support to Unity Tablets.

3. **Securus Local Platform (SLP):**

- Functions as a secure gateway, inspecting all network packets and governing content access.
- Blocks any unauthorized network traffic, ensuring complete control over accessible content.
- Only authorized devices are granted IP addresses for network connection.

Tablet Administration

• **Command & Control Officer Tablets:**

- Enable real-time application control by individual, group, or facility-wide levels.
- Dashboard provides analytics, search functions, and customizable staff permissions.
- Application restriction and behavior modification tools ensure compliance and facility safety.

• **SubManager App:**

- Allows staff to monitor user profiles, locations, permissions, and device usage, simplifying administration.

Content Review and Management

- Content—including movies, music, games, and educational material—is vetted by a dedicated Securus team and automated tools.
- Inappropriate content can be removed remotely to maintain corrections-appropriate standards.

Advantages of Securus Unity Tablets

- Enhanced security minimizes risks of contraband communication.
- Simplified distribution and administrative control improve facility efficiency.
- Free and premium content options promote rehabilitation and connection with families.

By combining advanced technology, strict security protocols, and user-focused content, Securus ensures that its tablet solutions provide optimal value while adhering to the highest industry standards.

Compliance and Support

Securus provides end-to-end support to ensure seamless implementation, operation, and management of the Unity Tablet Program. This includes:

1. **Deployment and Training:**
 - Expert support teams for initial deployment and onboarding.
 - Customized training for facility staff to operate Command & Control Tablets and the SubManager app effectively.
2. **Hardware Maintenance:**
 - Routine checks and updates to ensure optimal performance.
 - Replacement of end-of-life devices at no additional cost.
3. **Software Updates:**
 - Automatic, no-downtime updates delivered via Wi-Fi regularly, as needed, enhancing features and fixing any potential vulnerabilities.
4. **Performance Monitoring:**
 - Real-time monitoring of networks and devices to identify and address unusual activity.
 - Proactive customer notifications for potential security threats or breaches.
5. **Feedback and Improvement:**
 - Transactional and relationship surveys gather insights to refine and enhance program delivery.
 - User groups provide an ongoing forum for innovation based on customer feedback.

Tablet Features that Support Facility Objectives

1. **Inmate Engagement and Rehabilitation:**
 - Access to educational materials, job search resources, and self-help programs.
 - Premium content for entertainment improves quality of life and reduces idle time.
 - Communication tools strengthen family connections, supporting better reintegration outcomes.
2. **Operational Efficiency:**
 - Digitization of grievance processes and forms reduces administrative burdens and expedites resolution times.
 - Individual tablet assignment minimizes strain on networks and staff intervention compared to shared device models.
3. **Behavior Management:**
 - Customizable controls allow staff to modify access based on individual behavior, promoting compliance and rehabilitation.
 - Immediate response options for addressing misuse or security violations.
4. **Security and Integrity:**
 - Multiple layers of encryption and secure access prevent breaches.
 - Wi-Fi and charging solutions ensure limited interaction with external hardware or networks.

Securus Unity Tablets are not merely tools for entertainment or communication but represent a holistic approach to modernizing correctional facilities. By enhancing rehabilitation opportunities, streamlining

operations, and maintaining the highest security standards, Securus shall be a trusted partner in creating a safer, more efficient corrections environment.

Covert Alert and Advanced Monitoring Features

The NextGen SCP solution includes robust security and monitoring functionalities to enhance investigative capabilities within Denver's detention facilities. The **Covert Alert** and other advanced monitoring features enable real-time oversight of inmate communication while maintaining anonymity and operational flexibility.

Covert Alert Feature

The Covert Alert feature provides authorized personnel with the ability to monitor live calls in stealth mode, ensuring effective investigation of potentially illicit activities. Key functionalities include:

- **Automatic Call Forwarding:** Live calls can be forwarded to an investigator's designated phone number in listen-only mode.
- **Customizable Triggers:** Alerts can be configured for specific phone numbers, persons experiencing incarceration, or calls from specific terminals.
- **Remote Monitoring:** Calls can be monitored from any location via a phone or on-site workstations using the NextGen SCP Monitor Activity page.
- **Simultaneous Access:** Multiple investigators can listen to the same call in real time, enhancing collaborative investigative efforts.
- **Email Notifications:** Covert Alerts can send an email to investigators with details such as the date, time, inmate PIN, originating phone, and dialed number immediately after the called party accepts the call.

For added security, the Covert Alert feature can require investigators to input a PIN to access the call, with a customizable message prompting authentication.

Additional Capabilities

- **"Barge In" Functionality:** Investigators can interrupt a live call to communicate directly with the inmate and the called party or terminate the call by entering a specific code.
- **Call Detail Record Reports:** Comprehensive records of Covert Alert calls are available, including searchable fields for specific activities.
- **Silent Monitoring:** Using analog suppression/amplification technology, investigators can listen to calls without detection by either party.
- **Scan Patrol:** This feature allows users to cycle through active calls in brief intervals to identify relevant content for further review.

Integrated Call Recording and Monitoring

NextGen SCP includes an integrated recording system with advanced capabilities to support investigative processes:

- **Real-Time and Archived Access:** Personnel can monitor live calls and retrieve archived recordings via user-friendly interfaces.
- **Data Redundancy:** Recordings are stored in multiple secure data centers, ensuring reliability and redundancy.
- **Detailed Activity Logs:** Call monitoring includes features like adding notes, flagging calls, viewing recent activity, and accessing billing and usage details.
- **Remote Access:** Authorized users can access recordings and live call monitoring from approved devices with internet connectivity.

Disabling and Disconnecting Calls

Authorized users can manually or automatically disable telephones or groups of telephones based on preset schedules or as needed. This functionality ensures immediate control over communication activity while allowing flexibility in managing call operations.

Security and Compliance

NextGen SCP provides multiple layers of security to protect communication integrity and comply with regulatory requirements:

- Exclusion of private calls, such as those to legal counsel, from recording or monitoring.
- Advanced network security measures, including encryption, IP authentication, and access controls.

With these tools, the Covert Alert and monitoring features deliver an unparalleled level of control, security, and flexibility, ensuring Denver’s detention facilities can efficiently address safety concerns and operational needs.

eMessaging Application Pricing

Securus’ eMessaging Application (“eMessaging”) allows two-way electronic communication between friends, family, and incarcerated users. Users purchase eMessaging “stamps,” which fund message transmissions as outlined below:

Type of Message (When Available)	Number of Stamps	Notes
Text Message	1 stamp per message and/or up to 50 “connects” per message	
Photo	1 stamp per photo and/or up to 50 “connects” per photo	Limit of 5 photos per eMessage; 3 MB/photo limit
eCard	1 stamp per eCard and/or up to 50 “connects” per eCard	Limit of 5 eCards per eMessage
VideoGram	3 stamps per VideoGram and/or up to 150 “connects” per VideoGram	

Attachments may be combined within a single eMessage transmission.

Stamp Pricing

- Friends and family purchase facility-specific stamp books in the following quantities:

Number of Stamps	Price (Excluding Taxes and Fees)
5	\$1.25
10	\$2.50
20	\$5.00
50	\$12.50

- Incarcerated users may purchase stamps using funds in a Securus Debit account:

Number of Stamps	Price (Excluding Taxes and Fees)
1	\$0.25
2	\$0.50
5	\$1.25
10	\$2.50

Pricing Adjustments

Any pricing adjustment will be mutually agreed to between the parties.

Commission Payments

Contractor will pay the City a 25% commission on each redeemed stamp, based on the Stamp Book Price (excluding applicable taxes, fees, or surcharges) and in accordance with the Cost and Compensation section above.

Text Connect Application Pricing

Securus' Text Connect Application ("STC") enables two-way electronic communication via text messages (up to 160 characters per message) between friends, family, and incarcerated individuals.

Connect Package Pricing

Friends and family members purchase text packages, priced as follows:

Package Usage (Connects)	Base Package Price	Agency % of Base	Agency Charge Paid to the City	Transaction Fee	Total Package Price (Before Tax)	Base Price Per Text	Total Price Per Text (Before Tax)	Base Price Per eCard	Total Price Per eCard (Before Tax)
500	\$5.00	25%	\$1.25	\$3.75	\$10.00	\$0.10	\$0.20	\$0.20	\$0.40
1000	\$9.50	25%	\$2.38	\$3.75	\$15.63	\$0.10	\$0.16	\$0.19	\$0.31
2000	\$18.00	25%	\$4.50	\$3.75	\$26.25	\$0.09	\$0.13	\$0.18	\$0.26
4000	\$32.00	25%	\$8.00	\$3.75	\$43.75	\$0.08	\$0.11	\$0.16	\$0.22

Pricing Adjustments

Any pricing adjustment will be mutually agreed to between the parties.

Commission Payments

Contractor will pay the commission stated in the table immediately above in accordance with the Cost and Compensation section above.

Tablet Pricing

TABLETS:

Contractor will deploy free basic community tablets to the Facility. Additionally, personal rental tablets with premium content will be available for inmates.

Premium Content

Premium content may include, but is not limited to:

- Songs
- Games
- Movies
- Television episodes

Premium content availability is subject to change and may be governed by third-party licensing agreements. If the City provides content for display on the tablets, the City warrants that it has secured all necessary licenses and rights for such content. Contractor disclaims liability for third-party applications or external content published by the City.

Compensation

- **Promotional Tablet Rental Rate:** \$5.00 per tablet per month (plus applicable taxes, fees, and surcharges) for the initial 12-month period.

- **Commission:** the City will receive a 25% commission on revenue from tablet rentals and premium content purchases, net of licensing and network costs (excluding applicable taxes, fees, and surcharges in accordance with the Cost and Compensation section above).
- **Fee Payment Options:** Subscription and premium content fees can be paid via Securus Debit or Tablet User Accounts.

Note: After the initial 12-month period, Contractor and the City may renegotiate the promotional rental rate and/or commission structure if Contractor's tablet-related costs exceed revenue.

Earbuds

- **Price per Set:** \$5.66 (minimum order of 25 units, in increments of 25).
- **Order Fulfillment:** Contractor may decline orders not meeting these requirements.
- **City Resale Limit:** Earbuds may not be resold for more than \$19.99 per set without Contractor's approval.
- **Optional Facilitation:** Contractor will work with the City's commissary provider to facilitate earbud sales if requested.

Tablets Terms and Conditions

1. **City Warranty:**
 - City will not provide tablets to incarcerated individuals known to pose a threat or risk of dangerous or unauthorized tablet use.
2. **Nature of Premium Content Service:**
 - Premium content is rented and available only during the individual's incarceration at the Facility. It will not be available upon release.
3. **Use of Investigator Pro and Earbuds:**
 - Investigator Pro™ is certified for use only with Contractor's earbuds. Using alternative earbuds may reduce the effectiveness of voice identification technology.
 - City will refrain from selling or distributing earbuds with microphones other than Contractor's certified earbuds.
4. **Disclaimer of Warranties:**
 - Contractor disclaims all express or implied warranties, including merchantability or fitness for a particular purpose.
 - Contractor will not be liable for any indirect, incidental, or consequential damages related to tablet use or unavailability.

Investigatory Tools and Pricing

THREADS

THREADS enables authorized law enforcement users to analyze corrections and communications data from multiple sources to generate targeted investigative leads. It includes the following components:

- **Data Analysis**
- **Data Review**
- **Data Import**

THREADS includes a community feature that allows participating correctional facilities to access and analyze communications data shared within the THREADS community. The City has opted into this feature and acknowledges that data from its Facility or Facilities will be included in the shared dataset.

To ensure privacy and security, data shared within the THREADS community will only be accessible to authorized law enforcement users and strictly used for investigative purposes. The use, access, and dissemination of shared data must comply with all applicable privacy laws and regulations governing law enforcement investigations.

- **Fixed Cost:** \$1,800.00 per month, plus applicable taxes and fees.
-

Word Alert

Word Alert is a safety and investigative feature of the NextGen Secure Communications Platform. It uses speech-to-text technology to transcribe audio from calls and, if applicable, Video Connect sessions, enabling investigators to:

- Search text transcripts for specified words and phrases.
 - Request English translations of transcripts in other languages.
 - **Fixed Cost:** \$6,460.67 per month, plus applicable taxes and fees.
-

Investigator Pro

Investigator Pro uses continuous voice identification technology to:

- Identify incarcerated individuals speaking on calls.
- Detect three-way call violations.
- Generate investigative leads by analyzing voice correlations among calls.

Voice model enrollment for incarcerated individuals must be supervised and facilitated by the City.

- **Fixed Cost:** \$12,921.60 per month, plus applicable taxes and fees.
-

ICER

The ICER system detects intra- and inter-Facility communications between incarcerated individuals from multiple sources to generate targeted investigative leads.

- **Fixed Cost:** Provided at no charge to the City.
-

Guarded Exchange Services

Guarded Exchange analysts monitor Securus Video Connect sessions for protocol violations based on the City's scheduling preferences:

- **24-hour Notice Required:** All sessions monitored for violations.
- **Pop-Up Visitation:** At least one analyst monitors sessions during Video Connect hours, as feasible.

Guarded Exchange provides violation reports to the City.

- **Fixed Cost:** \$1,875.00 per month, plus applicable taxes and fees.

Securus Digital Mail Center

The Digital Mail Center provides a secure way to scan, manage, and deliver mail electronically to incarcerated recipients. Features include:

- Scanning and delivery of mail within 48 hours of receipt.
- Administrative tools for approval, rejection, and activity audits.
- Options to destroy or return undeliverable mail based on the City preferences.
- **Fixed Cost:** \$4,580.10 per month, plus applicable taxes and fees.

Fastcase Law Library

Fastcase provides industry-leading tools to make legal research easier and more intuitive:

- **Fixed Cost:** \$392.30 per month, plus applicable taxes and fees.

Terms of Use for Investigative Products and Features

1. **Compliance:** City is responsible for adhering to applicable laws, including privacy, consumer protection, and data security.
2. **Conditional Use:** Contractor reserves the right to modify or discontinue features if terms or legal requirements are violated.
3. **Transcription/Translation Accuracy:** Speech-to-text services are provided "AS IS" and may contain inaccuracies due to various factors.
4. **Disclaimer of Warranties:** All products and features are provided without express or implied warranties of any kind.
5. **Limitation of Liability:** Contractor's liability for any loss or injury related to the investigative products is capped at \$10,000.

This pricing and feature structure reflects Contractor's comprehensive investigative solutions tailored for facility security and compliance.

Fee Schedule.**All cost to the city are fixed and bill monthly**

	Monthly Cost	Annual Cost
THREADS	\$1,800	\$21,600
Word alert	\$6,460.67	\$77,528.04
Investigator Pro	\$12,921.60	\$155,059.20
Guarded exchange services	\$1,875	\$22,500
Digital Mail center	\$4,580.10	\$54,961.20
Fastcase Law Library	\$392.30	\$4,707.60
Total Costs	\$28,029.67	\$336,356.04

City received Commissions
25% commission from eMessaging
25% commission from tablet rentals and premium content
25% Commission from Text Connect

Optional pricing / costs items for Inmates

Calls	\$.06/minute		
Video visits	\$.11/minute		
eMessaging Stamps	\$0.25 per stamp (see table above)		
Text packages	Rates vary by amount purchased (see table above)		
Tablet rentals	\$5.00 per month for premium content		
Ear buds	5.56 After first provided pair at no cost		

Maximum Contract Breakdown.

Year	Revenue*	Expenditure (Base Payments)	Contingency	Total Expenditure
Year 1	\$190,000	\$336,356	\$65,000	\$401,356
Year 2	\$190,000	\$336,356	\$65,000	\$401,356
Year 3	\$190,000	\$336,356	\$65,000	\$401,356
Year 4	\$190,000	\$336,356	\$65,000	\$401,356
Year 5	\$190,000	\$336,356	\$65,000	\$401,356
Total	\$950,000	\$1,681,780	\$325,000	\$2,006,780

*Note – Revenue is estimated based on projected usage only. See Commission Schedule for rates.

Conclusion

This Scope of Work establishes the framework for the successful implementation and operation of the telephone, tablet, and video visitation system at Denver’s detention facilities. By leveraging Securus Technologies’ extensive experience, cutting-edge solutions, and commitment to service excellence, the City of Denver can ensure a secure, user-friendly, and future-ready communication platform for its detention system.

The proposed solution aligns with DSD’s mission to deliver services that support operational efficiency, safety, and the needs of individuals experiencing incarceration and their families.

Exhibit B - End-of-Contract Extraction

The terms and conditions of the Agreement will continue to apply for so long as Contractor continues to provide the Works to the City after the expiration or earlier termination of this Agreement. To ensure a seamless transition at the conclusion of the contract period, the Contractor shall provide comprehensive end-of-contract extraction services, including the following:

1. Inventory Assessment and Decommissioning Planning

- **Asset Inventory:** Compile a detailed inventory of all hardware and software deployed at the Downtown Detention Center (DDC) and County Jail (COJL), including telephones, kiosks, tablets, servers, switches, and other associated equipment.
- **EOL Identification:** Highlight any components nearing or exceeding end-of-life status for priority extraction.
- **Transition Plan:** Develop a structured extraction and decommissioning plan in collaboration with DSD stakeholders to minimize service disruption.

2. Data Retrieval and Migration

- **Data Backup:** Provide full backups of all system data, including call logs, visitation records, investigative tool reports, and analytics reports.
- **Data Migration Support:** Assist in securely transferring data to systems or vendors designated by DSD.
- **Data Integrity Verification:** Ensure the accuracy and completeness of all migrated data.

3. Hardware Removal

- **Systematic Decommissioning:**
 - Remove all telecommunication devices, kiosks, tablets, servers, and associated networking equipment.

Securely handle and dispose of any outdated or damaged hardware.

4. Software Deactivation and Archival

- **License Termination:** Deactivate all proprietary software and return any licenses to the vendor as required.

5. Exit Documentation

- **Exit Documentation:** Submit a comprehensive exit report detailing:
 - Assets removed and returned.
 - Data transferred or archived.
 - Any unresolved issues requiring further action.

6. Security and Compliance

- **Secure Extraction Process:** Implement strict security measures to protect sensitive data during the extraction process.
- **Regulatory Compliance:** Ensure that all activities adhere to applicable legal and operational standards, including retention requirements for records and data.

7. Post-Extraction Support

- **Support Period:** Provide a limited period of post-extraction support to address any unforeseen issues or questions.
- **Transition Liaison:** Designate a point of contact for coordinating with DSD and any successor vendors.

By including these end-of-contract extraction services, the SOW ensures that DSD is fully equipped to transition seamlessly while preserving operational continuity and compliance.

Exhibit C - Service Level Agreement (SLA)

This Service Level Agreement (“SLA”) defines the expectations and standards for Vendor Support programs and policies between the Provider and the Customer/Denver Sheriff Department.

1. Definitions

- **“Provider/Securus”** refers to the Vendor offering the services covered under this SLA.
 - **“Customer/Denver Sheriff Department”** refers to the party receiving the services outlined in this SLA.
 - **“Applications”** refers to the systems, software, or equipment provided by the Provider/Securus.
 - **“Outage”** means any interruption in the normal functionality of the Applications.
 - **“System Event”** refers to an outage or malfunction that requires attention or maintenance.
 - **“Technical Support”** refers to the Provider/Securus’s support team responsible for responding to and resolving System Events.
 - **“Priority Level”** refers to the classification of System Events based on their impact, as detailed in the Response and Resolution Goals section.
 - **“Response Time”** means the time within which the Provider/Securus acknowledges and begins addressing a reported System Event.
 - **“Resolution Time”** means the time taken to resolve a System Event fully.
 - **“System”** means Secure Call Platform, as better described in Exhibit A to the Agreement.
 - **“Workaround”** refers to a temporary solution to mitigate the impact of a System Event while a permanent fix is implemented.
-

2. Accessing Support

The Provider/Securus will offer multiple channels to assist the Customer/Denver Sheriff Department in resolving technical issues, including:

- **Online Support:** Accessible via a ticketing system.
 - **Phone Support:** Available through a dedicated support hotline.
 - **Escalation Contacts:** Additional contacts for unresolved issues or delayed responses.
-

3. Priority Levels and Response Goals

Priority Level	Description	Time to Initial Contact	Response Hours	Resolution Time	Resolution Goal
P1	Critical: >50% system degradation or a complete outage affecting core services, security breach or data loss.	Within 1 hour	24/7/365	Within 24 hours	Continuous work until resolved. Regular updates provided until full resolution or a Workaround is implemented.
P2	High: 25%-50% system degradation impacting operations, with no reasonable workaround available.	Within 4 business hours	24/7/365	Within 72 hours	Efforts to resolve or provide a Workaround within the specified timeframe. Regular updates provided.
P3	Medium: Minor issues or singular break/fix problems with available workarounds.	Within 1 business day	Business Hours (8 AM - 5 PM, MST)	Within 10 business days	Commercially reasonable efforts to resolve or implement a Workaround within the specified timeframe.

4. Escalation Path

If issues are not resolved within the stated response times, the following escalation path will be followed:

Tier	Support Type	Contact Method	Responsibilities
1	Customer/Denver Sheriff Department Super User(s)	TMU #dsddtu@denvergov.org (720)865-4388	Basic troubleshooting, user support, documenting issues, and escalating unresolved problems.
2	Customer/Denver Sheriff Department Application Support	TMU #dsddtu@denvergov.org (720)865-4388	Application administration, access management, troubleshooting, and escalation to Vendor.
3	Vendor Online Support	https://securus.my.site.com	Initial point of Vendor support, problem resolution, and coordinating third-party integrations.
4	Vendor Phone Support	Technical Support: (866) 558-2323 (Option 4) Family and Friends Customer Support: (800) 844-6591	24/7 support for critical issues and escalation for unresolved or complex problems.

5. Planned Outages

- **Notification:** The Customer/Denver Sheriff Department will be notified of planned outages at least 72 hours in advance.
- **Timing:** Planned outages will occur during non-critical business hours, typically after 6 PM local time.
- **Uptime Compliance:** Planned outages will be included in the uptime percentage calculation outlined in the Availability section.

6. Availability

- **Uptime Requirement:** The system must maintain at least 99.0% availability during each calendar month, including all components used for daily operations.
- **Calculation:** System Availability is calculated as:

(Total Minutes - Downtime Minutes) / Total Minutes x 100=Availability %

7. Service Credits & Termination

Service Credits

If the Provider (Securus) fails to meet the established Response or Resolution Goals outlined in this SLA, the Customer (Denver Sheriff Department) will be entitled to Service Credits. Service Credits will apply exclusively to the following services and products:

- Investigator Pro
- Guarded Exchange Services
- Securus Digital Mail Center
- Word Alert
- Threads

The Service Credits will be calculated based on the following thresholds of **System Availability**:

System Availability	Service Credit
< 99.0%	10%
< 95.0%	20%
< 90.0%	30%
< 85.0%	40%

Service Credits are calculated as a percentage of the fees associated with the affected services and will be applied as follows:

1. **Credit to Future Invoices:** Service Credits will reduce the amount due on the Customer's future invoices.
2. **Refund of Prepaid Fees:** For prepaid fees, Service Credits will be issued as a refund, where applicable.

Service Credits are intended to acknowledge and address service deficiencies and to incentivize the Provider to meet performance expectations. However, Service Credits are not designed to serve as a full remedy for any operational, reputational, or financial losses incurred by the Customer due to such deficiencies.

Termination

The Customer (Denver Sheriff Department) may terminate the Agreement **without penalty** under the following circumstances:

- The Provider fails to meet SLA obligations for **three consecutive months**.

- The Provider fails to meet SLA obligations for **five non-consecutive months within a calendar year**.

In the event of termination under these conditions, the Provider (Securus) will refund the Customer a **pro-rata portion of any prepaid fees** that cover the remaining term of the Agreement.

Termination rights outlined in this section do not limit or waive any other legal remedies available to the Customer under applicable laws or the terms of this Agreement.

8. Miscellaneous

- **Monitoring:** The Provider/Securus will monitor its systems 24/7 to identify and address issues proactively.
- **Compliance Inquiries:** The Customer/Denver Sheriff Department may request evidence of SLA compliance at any time.

EXHIBIT D
BUSINESS ASSOCIATE AGREEMENT
HIPAA/HITECH

1. GENERAL PROVISIONS AND RECITALS.

- 1.01 The parties agree that the terms used, but not otherwise defined below, shall have the same meaning given to such terms under the Health Insurance Portability and Accountability Act of 1996, Public Law 104-191 ("HIPAA"), the Health Information Technology for Economic and Clinical Health Act, Public Law 111-005 ("the HITECH Act"), and their implementing regulations at 45 CFR Parts 160 and 164 ("the HIPAA regulations") as they exist or may hereafter be amended.
- 1.02 The parties agree that a business associate relationship (as described in 45 CFR §160.103) under HIPAA, the HITECH Act, and the HIPAA regulations arises between the CONTRACTOR and the CITY to the extent that CONTRACTOR performs, or delegates to subcontractors to perform, functions or activities on behalf of CITY.
- 1.03 CITY wishes to disclose to CONTRACTOR certain information, some of which may constitute Protected Health Information ("PHI") as defined below, to be used or disclosed in the course of providing services and activities.
- 1.04 The parties intend to protect the privacy and provide for the security of PHI that may be created, received, maintained, transmitted, used, or disclosed pursuant to the Agreement in compliance with the applicable standards, implementation specifications, and requirements of HIPAA, the HITECH Act, and the HIPAA regulations as they exist or may hereafter be amended.
- 1.05 The parties understand and acknowledge that HIPAA, the HITECH Act, and the HIPAA regulations do not pre-empt any state statutes, rules, or regulations that impose more stringent requirements with respect to privacy of PHI.
- 1.06 The parties understand that the HIPAA Privacy and Security rules apply to the CONTRACTOR in the same manner as they apply to a covered entity. CONTRACTOR agrees to comply at all times with the terms of this Agreement and the applicable standards, implementation specifications, and requirements of the Privacy and the Security rules, as they exist or may hereafter be amended, with respect to PHI.

2. DEFINITIONS.

- 2.01 "Administrative Safeguards" are administrative actions, and policies and procedures, to manage the selection, development, implementation, and maintenance of security measures to protect electronic PHI and to manage the conduct of CONTRACTOR's workforce in relation to the protection of that information.
- 2.02 "Agreement" means the attached Agreement and its exhibits to which these additional terms are incorporated by reference.
- 2.03 "Breach" means the acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule which compromises the security or privacy of the PHI.

2.03.1 Breach excludes:

1. Any unintentional acquisition, access, or use of PHI by a workforce member or person acting under the authority of CONTRACTOR or CITY, if such acquisition, access, or use was made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under the Privacy Rule.
2. Any inadvertent disclosure by a person who is authorized to access PHI to another person authorized to access PHI, or organized health care arrangement in which CITY participates, and the information received as a result of such disclosure is not further used or disclosed in a manner disallowed under the HIPAA Privacy Rule.
3. A disclosure of PHI where CONTRACTOR or CITY has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

2.03.2 Except as provided in paragraph (a) of this definition, an acquisition, access, use, or disclosure of PHI in a manner not permitted under the HIPAA Privacy Rule is presumed to be a breach unless CONTRACTOR demonstrates that there is a low probability that the PHI has been compromised based on a risk assessment of at least the following factors:

1. The nature and extent of the PHI involved, including the types of identifiers and the likelihood of re-identification;
2. The unauthorized person who used the PHI or to whom the disclosure was made;
3. Whether the PHI was actually acquired or viewed; and
4. The extent to which the risk to the PHI has been mitigated.

2.04 "CONTRACTOR" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.05 "CITY" shall have the same meaning as in the attached Agreement, to which these Business Associate terms are incorporated by reference.

2.06 "Data Aggregation" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.07 "Designated Record Set" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.08 "Disclosure" shall have the meaning given to such term under the HIPAA regulations in 45 CFR §160.103.

2.09 "Health Care Operations" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §164.501.

2.10 "Immediately" where used here shall mean within 24 hours of discovery.

- 2.11 "Individual" shall have the meaning given to such term under the HIPAA Privacy Rule in 45 CFR §160.103 and shall include a person who qualifies as a personal representative in accordance with 45 CFR §164.502(g).
- 2.12 "Parties" shall mean "CONTRACTOR" and "CITY", collectively.
- 2.13 "Physical Safeguards" are physical measures, policies, and procedures to protect CONTRACTOR's electronic information systems and related buildings and equipment, from natural and environmental hazards, and unauthorized intrusion.
- 2.14 "The HIPAA 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.
- 2.15 "Protected Health Information" or "PHI" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.
- 2.16 "Required by Law" shall have the meaning given to such term under the HIPAA Privacy Rule at 45 CFR §164.103.
- 2.17 "Secretary" shall mean the Secretary of the Department of Health and Human Services or his or her designee.
- 2.18 "Security Incident" means attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system. "Security incident" does not include trivial incidents that occur on a daily basis, such as scans, "pings", or unsuccessful attempts to penetrate computer networks or servers maintained by CONTRACTOR.
- 2.19 "The HIPAA Security Rule" shall mean the Security Standards for the Protection of electronic PHI at 45 CFR Part 160, Part 162, and Part 164, Subparts A and C.
- 2.20 "Subcontractor" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.
- 2.21 "Technical safeguards" means the technology and the policy and procedures for its use that protect electronic PHI and control access to it.
- 2.22 "Unsecured PHI" or "PHI that is unsecured" means PHI that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary of Health and Human Services ("HHS") in the guidance issued on the HHS Web site.
- 2.23 "Use" shall have the meaning given to such term under the HIPAA regulations at 45 CFR §160.103.

3. OBLIGATIONS AND ACTIVITIES OF CONTRACTOR AS BUSINESS ASSOCIATE.

- 3.01 CONTRACTOR agrees not to use or further disclose PHI that CITY discloses to CONTRACTOR except as permitted or required by this Agreement or by law.

- 3.02 CONTRACTOR agrees to use appropriate safeguards, as provided for in this Agreement, to prevent use or disclosure of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY, except as provided for by this Contract.
- 3.03 CONTRACTOR agrees to comply with the HIPAA Security Rule, at Subpart C of 45 CFR Part 164, with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits, on behalf of CITY.
- 3.04 CONTRACTOR agrees to mitigate, to the extent practicable, any harmful effect of a Use or Disclosure of PHI by CONTRACTOR in violation of the requirements of this Agreement that becomes known to CONTRACTOR.
- 3.05 CONTRACTOR agrees to immediately report to CITY any Use or Disclosure of PHI not provided for by this Agreement that CONTRACTOR becomes aware of. CONTRACTOR must report Breaches of Unsecured PHI in accordance with 45 CFR §164.410.
- 3.06 CONTRACTOR agrees to ensure that any of its subcontractors that create, receive, maintain, or transmit, PHI on behalf of CONTRACTOR agree to comply with the applicable requirements of Section 164 Part C by entering into a contract or other arrangement.
- 3.07 To comply with the requirements of 45 CFR §164.524, CONTRACTOR agrees to provide access to CITY, or to an individual as directed by CITY, to PHI in a Designated Record Set within fifteen (15) calendar days of receipt of a written request by CITY.
- 3.08 CONTRACTOR agrees to make amendment(s) to PHI in a Designated Record Set that CITY directs or agrees to, pursuant to 45 CFR §164.526, at the request of CITY or an Individual, within thirty (30) calendar days of receipt of the request by CITY. CONTRACTOR agrees to notify CITY in writing no later than ten (10) calendar days after the amendment is completed.
- 3.09 CONTRACTOR agrees to make internal practices, books, and records, including policies and procedures, relating to the use and disclosure of PHI received from, or created or received by CONTRACTOR on behalf of CITY, available to CITY and the Secretary in a time and manner as determined by CITY, or as designated by the Secretary, for purposes of the Secretary determining CITY'S compliance with the HIPAA Privacy Rule.
- 3.10 CONTRACTOR agrees to document any Disclosures of PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY, and to make information related to such Disclosures available as would be required for CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.
- 3.11 CONTRACTOR agrees to provide CITY information in a time and manner to be determined by CITY in order to permit CITY to respond to a request by an Individual for an accounting of Disclosures of PHI in accordance with 45 CFR §164.528.
- 3.12 CONTRACTOR agrees that, to the extent CONTRACTOR carries out CITY's obligation(s) under the HIPAA Privacy and/or Security rules, CONTRACTOR will comply with the requirements of 45 CFR Part 164 that apply to CITY in the performance of such obligation(s).

- 3.13 CONTRACTOR shall work with CITY upon notification by CONTRACTOR to CITY of a Breach to properly determine if any Breach exclusions exist as defined below.

4. SECURITY RULE.

- 4.01 CONTRACTOR shall comply with the requirements of 45 CFR § 164.306 and establish and maintain appropriate Administrative, Physical and Technical Safeguards in accordance with 45 CFR §164.308, §164.310, §164.312, §164.314 and §164.316 with respect to electronic PHI that CITY discloses to CONTRACTOR or that CONTRACTOR creates, receives, maintains, or transmits on behalf of CITY. CONTRACTOR shall follow generally accepted system security principles and the requirements of the HIPAA Security Rule pertaining to the security of electronic PHI.
- 4.02 CONTRACTOR shall ensure that any subcontractors that create, receive, maintain, or transmit electronic PHI on behalf of CONTRACTOR agree through a contract with CONTRACTOR to the same restrictions and requirements contained here.
- 4.03 CONTRACTOR shall immediately report to CITY any Security Incident of which it becomes aware. CONTRACTOR shall report Breaches of Unsecured PHI as described in 5. BREACH DISCOVERY AND NOTIFICATION below and as required by 45 CFR §164.410.

5. BREACH DISCOVERY AND NOTIFICATION.

- 5.01 Following the discovery of a Breach of Unsecured PHI, CONTRACTOR shall notify CITY of such Breach, however, both parties may agree to a delay in the notification if so advised by a law enforcement official pursuant to 45 CFR §164.412.
- 5.01.1 A Breach shall be treated as discovered by CONTRACTOR as of the first day on which such Breach is known to CONTRACTOR or, by exercising reasonable diligence, would have been known to CONTRACTOR.
- 5.01.2 CONTRACTOR shall be deemed to have knowledge of a Breach, if the Breach is known, or by exercising reasonable diligence would have been known, to any person who is an employee, officer, or other agent of CONTRACTOR, as determined by the federal common law of agency.
- 5.02 CONTRACTOR shall provide the notification of the Breach immediately to the CITY DEH Executive Director or other designee.
- 5.02.1 CONTRACTOR'S initial notification may be oral, but shall be followed by written notification within 24 hours of the oral notification.
- 5.03 CONTRACTOR'S notification shall include, to the extent possible:
- 5.03.1 The identification of each Individual whose Unsecured PHI has been, or is reasonably believed by CONTRACTOR to have been, accessed, acquired, used, or disclosed during the Breach;
- 5.03.2 Any other information that CITY is required to include in the notification to each Individual under 45 CFR §164.404 (c) at the time CONTRACTOR is required to notify CITY, or

promptly thereafter as this information becomes available, even after the regulatory sixty (60) day period set forth in 45 CFR §164.410 (b) has elapsed, including:

1. A brief description of what happened, including the date of the Breach and the date of the discovery of the Breach, if known;
2. A description of the types of Unsecured PHI that were involved in the Breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);
3. Any steps Individuals should take to protect themselves from potential harm resulting from the Breach;
4. A brief description of what CONTRACTOR is doing to investigate the Breach, to mitigate harm to Individuals, and to protect against any future Breaches; and
5. Contact procedures for Individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

- 5.04 CITY may require CONTRACTOR to provide notice to the Individual as required in 45 CFR §164.404, if at the sole discretion of the CITY, it is reasonable to do so under the circumstances.
- 5.05 In the event that CONTRACTOR is responsible for a Breach of Unsecured PHI in violation of the HIPAA Privacy Rule, CONTRACTOR shall have the burden of demonstrating that CONTRACTOR made all required notifications to CITY, and as required by the Breach notification regulations, or, in the alternative, that the acquisition, access, use, or disclosure of PHI did not constitute a Breach.
- 5.06 CONTRACTOR shall maintain documentation of all required notifications of a Breach or its risk assessment under 45 CFR §164.402 to demonstrate that a Breach did not occur.
- 5.07 CONTRACTOR shall provide to CITY all specific and pertinent information about the Breach, including the information listed above, if not yet provided, to permit CITY to meet its notification obligations under Subpart D of 45 CFR Part 164 as soon as practicable, but in no event later than fifteen (15) calendar days after CONTRACTOR's initial report of the Breach to CITY.
- 5.08 CONTRACTOR shall continue to provide all additional pertinent information about the Breach to CITY as it becomes available, in reporting increments of five (5) business days after the prior report to CITY. CONTRACTOR shall also respond in good faith to all reasonable requests for further information, or follow-up information, after report to CITY, when such request is made by CITY.
- 5.09 In addition to the provisions in the body of the Agreement, CONTRACTOR shall also bear all expense or other costs associated with the Breach and shall reimburse CITY for all expenses CITY incurs in addressing the Breach and consequences thereof, including costs of investigation, notification, remediation, documentation or other costs or expenses associated with addressing the Breach.

6. PERMITTED USES AND DISCLOSURES BY CONTRACTOR.

- 6.01 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR as necessary to perform functions, activities, or services for, or on behalf of, CITY as specified in the Agreement, provided that such use or Disclosure would not violate the HIPAA Privacy Rule if done by CITY.
- 6.02 CONTRACTOR may use PHI that CITY discloses to CONTRACTOR, if necessary, for the proper management and administration of the Agreement.
- 6.03 CONTRACTOR may disclose PHI that CITY discloses to CONTRACTOR to carry out the legal responsibilities of CONTRACTOR, if:
 - 6.03.1 The Disclosure is required by law; or
 - 6.03.2 CONTRACTOR obtains reasonable assurances from the person or entity to whom/which the PHI is disclosed that it will be held confidentially and used or further disclosed only as required by law or for the purposes for which it was disclosed to the person or entity and the person or entity immediately notifies CONTRACTOR of any instance of which it is aware in which the confidentiality of the information has been breached.
- 6.04 CONTRACTOR may use or further disclose PHI that CITY discloses to CONTRACTOR to provide Data Aggregation services relating to the Health Care Operations of CONTRACTOR.
- 6.05 CONTRACTOR may use and disclose PHI that CITY discloses to CONTRACTOR consistent with the minimum necessary policies and procedures of CITY.

7. OBLIGATIONS OF CITY.

- 7.01 CITY shall notify CONTRACTOR of any limitation(s) in CITY'S notice of privacy practices in accordance with 45 CFR §164.520, to the extent that such limitation may affect CONTRACTOR'S Use or Disclosure of PHI.
- 7.02 CITY shall notify CONTRACTOR of any changes in, or revocation of, the permission by an Individual to use or disclose his or her PHI, to the extent that such changes may affect CONTRACTOR'S Use or Disclosure of PHI.
- 7.03 CITY shall notify CONTRACTOR of any restriction to the Use or Disclosure of PHI that CITY has agreed to in accordance with 45 CFR §164.522, to the extent that such restriction may affect CONTRACTOR'S use or disclosure of PHI.
- 7.04 CITY shall not request CONTRACTOR to use or disclose PHI in any manner that would not be permissible under the HIPAA Privacy Rule if done by CITY.

8. BUSINESS ASSOCIATE TERMINATION.

- 8.01 Upon CITY'S knowledge of a material breach or violation by CONTRACTOR of the requirements of this Contract, CITY shall:

8.01.1 Provide an opportunity for CONTRACTOR to cure the material breach or end the violation within thirty (30) business days; or

8.01.2 Immediately terminate the Agreement, if CONTRACTOR is unwilling or unable to cure the material breach or end the violation within (30) days, provided termination of the Agreement is feasible.

8.02 Upon termination of the Agreement, CONTRACTOR shall either destroy or return to CITY all PHI CONTRACTOR received from CITY and any and all PHI that CONTRACTOR created, maintained, or received on behalf of CITY in conformity with the HIPAA Privacy Rule.

8.02.1 This provision shall apply to all PHI that is in the possession of subcontractors or agents of CONTRACTOR.

8.02.2 CONTRACTOR shall retain no copies of the PHI.

8.02.3 In the event that CONTRACTOR determines that returning or destroying the PHI is not feasible, CONTRACTOR shall provide to CITY notification of the conditions that make return or destruction infeasible. Upon determination by CITY that return or destruction of PHI is infeasible, CONTRACTOR shall extend the protections of this Agreement to the PHI and limit further Uses and Disclosures of the PHI to those purposes that make the return or destruction infeasible, for as long as CONTRACTOR maintains the PHI.

8.03 The obligations of this Agreement shall survive the termination of the Agreement.

9. SUBSTANCE ABUSE (42 C.F.R., Part 2).

CONTRACTOR shall also comply with all provisions of 42 C.F.R., Part 2 relating to substance abuse treatment and records.

EXHIBIT E - FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM

The goal of this document is to augment the CJIS Security Policy to ensure adequate security is provided for criminal justice systems while (1) under the control or management of a private entity or (2) connectivity to FBI CJIS Systems has been provided to a private entity (contractor). Adequate security is defined in Office of Management and Budget Circular A-130 as “security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information.”

The intent of this Security Addendum is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

This Security Addendum identifies the duties and responsibilities with respect to the installation and maintenance of adequate internal controls within the contractual relationship so that the security and integrity of the FBI’s information resources are not compromised. The security program shall include consideration of personnel security, site security, system security, and data security, and technical security.

The provisions of this Security Addendum apply to all personnel, systems, networks and support facilities supporting and/or acting on behalf of the government agency.

1.00 Definitions

1.01 Contracting Government Agency (CGA) – the government agency, whether a Criminal Justice Agency or a Noncriminal Justice Agency, which enters into an agreement with a private contractor subject to this Security Addendum.

1.02 Contractor – a private business, organization or individual which has entered into an agreement for the administration of criminal justice with a Criminal Justice Agency or a Noncriminal Justice Agency.

2.00 Responsibilities of the Contracting Government Agency.

2.01 The CGA will ensure that each Contractor employee receives a copy of the Security Addendum and the CJIS Security Policy and executes an acknowledgment of such receipt and the contents of the Security Addendum. The signed acknowledgments shall remain in the possession of the CGA and available for audit purposes. The acknowledgement may be signed by hand or via digital signature (see glossary for definition of digital signature).

3.00 Responsibilities of the Contractor.

3.01 The Contractor will maintain a security program consistent with federal and state laws, regulations, and standards (including the CJIS Security Policy in effect when the contract is executed and all subsequent versions), as well as with policies and standards established by the Criminal Justice Information Services (CJIS) Advisory Policy Board (APB).

4.00 Security Violations.

4.01 The CGA must report security violations to the CJIS Systems Officer (CSO) and the Director, FBI, along with indications of actions taken by the CGA and Contractor.

4.02 Security violations can justify termination of the appended agreement.

4.03 Upon notification, the FBI reserves the right to:

- a. Investigate or decline to investigate any report of unauthorized use;
- b. Suspend or terminate access and services, including telecommunications links. The FBI will provide the CSO with timely written notice of the suspension. Access and services will be reinstated only after satisfactory assurances have been provided to the FBI by the CGA and Contractor. Upon termination, the Contractor's records containing CHRI must be deleted or returned to the CGA.

5.00 Audit

5.01 The FBI is authorized to perform a final audit of the Contractor's systems after termination of the Security Addendum.

6.00 Scope and Authority

6.01 This Security Addendum does not confer, grant, or authorize any rights, privileges, or obligations on any persons other than the Contractor, CGA, CJA (where applicable), CSA, and FBI.

6.02 The following documents are incorporated by reference and made part of this agreement: (1) the Security Addendum; (2) the NCIC 2000 Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20. The parties are also subject to applicable federal and state laws and regulations.

6.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they augment the provisions of the CJIS Security Policy to provide a minimum basis for the security of the system and contained information and it is understood that there may be terms and conditions of the appended Agreement which impose more stringent requirements upon the Contractor.

6.04 This Security Addendum may only be modified by the FBI, and may not be modified by the parties to the appended Agreement without the consent of the FBI.

6.05 All notices and correspondence shall be forwarded by First Class mail to:

Information Security Officer

Criminal Justice Information Services Division, FBI

1000 Custer Hollow Road

Clarksburg, West Virginia 26306

**FEDERAL BUREAU OF INVESTIGATION
CRIMINAL JUSTICE INFORMATION SERVICES
SECURITY ADDENDUM**

CERTIFICATION

I hereby certify that I am familiar with the contents of (1) the Security Addendum, including its legal authority and purpose; (2) the NCIC Operating Manual; (3) the CJIS Security Policy; and (4) Title 28, Code of Federal Regulations, Part 20, and agree to be bound by their provisions.

I recognize that criminal history record information and related data, by its very nature, is sensitive and has potential for great harm if misused. I acknowledge that access to criminal history record information and related data is therefore limited to the purpose(s) for which a government agency has entered into the contract incorporating this Security Addendum. I understand that misuse of the system by, among other things: accessing it without authorization; accessing it by exceeding authorization; accessing it for an improper purpose; using, disseminating or re-disseminating information received as a result of this contract for a purpose other than that envisioned by the contract, may subject me to administrative and criminal penalties. I understand that accessing the system for an appropriate purpose and then using, disseminating or re-disseminating the information received for another purpose other than execution of the contract also constitutes misuse. I further understand that the occurrence of misuse does not depend upon whether or not I receive additional compensation for such authorized activity. Such exposure for misuse includes, but is not limited to, suspension or loss of employment and prosecution for state and federal crimes.

Printed Name/Signature of Contractor Employee

Date

Printed Name/Signature of Contractor Representative

Date

Organization and Title of Contractor Representative

EXHIBIT F, INFORMATION TECHNOLOGY PROVISIONS

This Exhibit regarding Information Technology Provisions (this “Exhibit”) is a material part of the Agreement between the Parties to which this Exhibit is attached. In addition to the requirements of the main body of this Agreement, the Contractor shall protect the City’s information technology resources and City Data in accordance with this Exhibit. All provisions of this Exhibit that refer to the Contractor shall apply equally to any Subcontractor performing work in connection with this Agreement. Unless the context clearly requires a distinction between the Agreement and this Exhibit, all references to “Agreement” shall include this Exhibit.

1. TECHNOLOGY SERVICES SPECIFICATIONS

- 1.1. User ID Credentials:** Internal corporate or customer (tenant) user account credentials shall be restricted, ensuring appropriate identity, entitlement, and access management and in accordance with established policies and procedures, as follows:
 - 1.1.1.** Identity trust verification and service-to-service application (API) and information processing interoperability (e.g., SSO and Federation);
 - 1.1.2.** Account credential lifecycle management from instantiation through revocation;
 - 1.1.3.** Account credential and/or identity store minimization or re-use when feasible; and
 - 1.1.4.** Adherence to industry acceptable and/or regulatory compliant authentication, authorization, and accounting (AAA) rules (e.g., strong/multi-factor, expire able, non-shared authentication secrets).
- 1.2. Identity Management:** The City’s Identity and Access Management (“IdM”) system is an integrated infrastructure solution that enables many of the City’s services and online resources to operate more efficiently, effectively, and securely. All new and proposed applications must utilize the authentication and authorization functions and components of an industry standard system. Strong authentication is required for privileged accounts or accounts with access to sensitive information. This technical requirement applies to all solutions regardless of where the application is hosted.
- 1.3. Supported Releases:** The Contractor shall maintain the currency of all third-party software used in the development and execution or use of the Work with third-party vendor approved and supported releases, including, but not limited to, all code libraries, frameworks, components, and other products (e.g., Java JRE, code signing certificates, .NET, jQuery plugins, etc.), whether commercial, free, open-source, or closed-source. This includes any of the Contractor’s controlled systems running on the City’s network, including, but not limited to, any application, firewall, or other type of physical or virtual appliances.
- 1.4. Updates & Upgrades:** During the Term of this Agreement, the Contractor shall provide the City with copies of all new versions, updates, and upgrades of the On-Premise Software (collectively, “Upgrades”), without additional charge, promptly after commercial release. Upon delivery to the City, Upgrades will become part of the On-Premise Software and will be subject to the license and other terms of this Agreement applicable to such On-Premise Software. In addition, the

Contractor shall ensure that SaaS receives all updates and upgrades the Contractor provides to its customers generally.

- 1.5. **Compatibility with Third-Party Software:** The Contractor acknowledges and agrees that the Work must integrate and operate compatibly with various third-party software products. The Contractor shall actively monitor and stay current on new version releases, updates, and changes made to any such third-party software that interfaces or integrates with the Contractor's Work. The Contractor shall ensure that its own products remain fully compatible with the most recent generally available versions of these third-party software components. Within ninety (90) days of the commercial release of a new generally available version of any interfacing third-party software, the Contractor shall complete all necessary testing, coding, and product updates to certify compatibility with the new version. The Contractor shall provide the updated and version-compatible products to the City at no additional cost. If the Contractor's Work is not compatible with the most current generally available third-party software versions required for operation, the City reserves the right to temporarily cease using the incompatible Work until the compatibility issue is resolved, without penalty or payment for a period of noncompliance. Under no circumstances shall the Contractor require the City to run old, non-current versions of third-party software to remain compatible with the Contractor's Work. The responsibility and costs for ensuring third-party software version compatibility shall reside solely with the Contractor.
- 1.6. **Adjustment of Licenses:** The City may, at each anniversary date of this Agreement, increase or decrease the number of licenses it has purchased under this Agreement by giving written notice to the Contractor at least thirty (30) days prior to the anniversary date. The Contractor shall adjust the invoice for the next billing period based on the unit price per license specified in this Agreement. The City shall not reduce the number of licenses below the minimum quantity required under this Agreement.
- 1.7. **Timing of Fees and Subscriptions:** Notwithstanding any provision to the contrary: (i) no fees for maintenance of On-Premise Software or SaaS, including without limitation for Upgrades, will accrue before Go-Live (as defined below); and (ii) no period before Go-Live will be counted against the time covered by any maintenance period. In addition, no fees for use of SaaS will accrue before Go-Live, and no period before Go-Live will be counted against the time covered by any SaaS subscription fees. "Go-Live" refers to the earlier of Acceptance of the On-Premise Software or SaaS or the City's first use of the On-Premise Software or SaaS in production, other than a beta use or trial.
- 1.8. **Performance Outside of the United States:** The Contractor shall request written approval from the City to perform, or subcontract to perform, Services outside the United States. The City may approve or deny such request within the City's sole discretion. Any notice or term in any Exhibit provided to the City by the Contractor regarding performance outside the United States shall be deemed ineffective and void if the City has not granted prior written approval for such performance. This prohibition shall also apply to using, processing, transmitting, or maintaining City Data outside of the United States. Notwithstanding anything to the contrary contained in the Agreement, the City shall have no responsibility or obligation to comply with foreign data

protection laws or policies, including, but not limited to, the General Data Protection Regulation of the European Union.

1.9. Continuity of Critical Services: The Contractor acknowledges that the Work to be performed under this Agreement is vital to the City and must be continued without interruption and that, upon this Agreement's expiration without renewal, a successor, either the City or another contractor, may continue them. The Contractor agrees to: (i) furnish phase-in training; and (ii) exercise its best efforts and cooperation to complete an orderly and efficient transition to a successor. The Contractor shall, upon the City's written notice: (i) furnish phase-in, phase-out services for up to sixty (60) days after this Agreement expires; and (ii) negotiate in good faith to determine the nature and extent of phase-in, phase-out services required. The Contractor shall provide sufficient experienced personnel during the phase-in, phase-out period to ensure that the Work called for by this Agreement are maintained at the required level of proficiency. The Contractor shall be reimbursed for all reasonable phase-in, phase-out costs (i.e., costs incurred within the agreed period after expiration that result from phase-in, phase-out operations) at the rates contained herein. The City shall have the authority extend this Agreement monthly if additional time is required beyond the termination of this Agreement, if necessary, to effectuate the transition, and the City shall pay a proration of the subscription fee during any necessary extension.

2. SECURITY AUDITS

2.1. Performance of Security Audits: Prior to the Effective Date of this Agreement, the Contractor, will at its expense conduct or have conducted the following, and thereafter, the Contractor will at its expense conduct or have conducted the following at least once per year, and immediately after any actual or reasonably suspected Security Breach: (i) upon execution of an NDA, a SSAE 18/SOC 2 Type 2 or other mutually agreed upon audit of the Contractor's security policies, procedures and controls; (ii) an annual external and internal vulnerability scan of the Contractor's systems and facilities, to include public facing websites, that are used in any way to deliver Services under this Agreement. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high; and (iii) an annual formal penetration test performed by qualified personnel of the Contractor's systems and facilities that are used in any way to deliver Work under this Agreement. The Contractor will provide the City the results of the above audits. The Contractor shall also protect data against deterioration or degradation of quality and authenticity by, at minimum, having a third party perform annual data integrity audits. In addition, the Contractor shall comply with the City's annual risk assessment and the results thereof.

2.2. Security Audit Results: The Contractor will provide the City the reports or other documentation resulting from the above audits, certifications, scans, and tests within seven (7) business days of the Contractor's receipt of such results. The report must include the vulnerability, age, and remediation plan for all issues identified as critical or high. Based on the results and recommendations of the above audits, the Contractor will, within thirty (30) calendar days of receipt of such results, promptly modify its security measures to meet its obligations under this

Agreement and provide the City with written evidence of remediation. The City may require, at the Contractor's expense, that the Contractor perform additional audits and tests, the results of which will be provided to the City within seven (7) business days of Contractor's receipt of such results. To the extent the Contractor controls or maintains information systems used in connection with this Agreement, the Contractor shall provide the City with the results of all security assessment activities when conducted on such information systems, including any code-level vulnerability scans, application-level risk assessments, and other security assessment activities as required by this Agreement or reasonably requested by the City. The Contractor will remediate any vulnerabilities to comply with its obligations hereunder. If additional funds are required to perform the tests required by the City that are not accounted for in this Agreement, the Parties agree to amend this Agreement as necessary.

3. DATA MANAGEMENT AND SECURITY

- 3.1. Compliance with Data Protection Laws and Policies:** In addition to the compliance obligations imposed by this Agreement, the Contractor shall comply with all information security and privacy obligations imposed by any federal, state, or local statute or regulation, or by any specifically incorporated industry standards or guidelines, as applicable to the Contractor under this Agreement, including, without limitation, applicable industry standards or guidelines based on the data's classification relevant to the Contractor's performance hereunder. If the Contractor becomes aware that it cannot reasonably comply with the terms or conditions contained herein due to a conflicting law or policy, the Contractor shall promptly notify the City.
- 3.2. Data Ownership:** Unless otherwise required by law, the City has exclusive ownership of all City Data under this Agreement, and the Contractor shall have no right, title, or interest in City Data. The Parties recognize and agree that the Contractor is a bailee for hire with respect to City Data. The Contractor's use and possession of City Data is solely on the City's behalf, and the Contractor shall only use City Data solely for the purpose of performing its obligations hereunder and shall not use City Data in the development of machine learning and artificial intelligence models for any purpose without the City's written consent. The City retains the right to access and retrieve City Data stored on the Contractor's infrastructure at any time during the Term. All City Data created and/or processed by the Work, if any, is and shall remain the property of the City and shall in no way become attached to the Work. This Agreement does not give a Party any rights, implied or otherwise, to the other's data, content, or intellectual property, except as expressly stated in this Agreement.
- 3.3. Data Access and Integrity:** The Contractor shall implement and maintain all appropriate administrative, physical, technical, and procedural safeguards necessary and appropriate to ensure compliance with the applicable law and regulation as they relate to the Contractor's performance hereunder to ensure the security and confidentiality of City Data. The Contractor shall protect against threats or hazards to the security or integrity of data; protect against unauthorized disclosure, access to, or use of data; restrict access to data as necessary; and ensure the proper and legal use of data. The Contractor shall provide the City with access, subject to the Contractor's reasonable security requirements, for purposes of inspecting and monitoring access and use of

City Data and evaluating security control effectiveness. The Contractor shall not engage in “data mining” except as specifically and expressly required by law or authorized in writing by the City. Upon written request, the Contractor shall provide the City its policies and procedures to maintain the confidentiality of City Data.

- 3.4. **Response to Legal Orders for City Data:** If the Contractor is required by a court of competent jurisdiction or administrative body to disclose City Data, the Contractor shall first notify the City and, prior to any disclosure, cooperate with the City’s reasonable requests in connection with the City’s right to intervene, quash, or modify the legal order, demand, or request, and upon request, provide the City with a copy of its response. Upon notice, the City will promptly coordinate with the Contractor regarding the preservation and disposition of any City Data and records relevant to any current or anticipated litigation. If the City receives a subpoena, legal order, or other legal demand seeking data maintained by the Contractor, the City will promptly provide a copy to the Contractor. Upon notice and if required by law, the Contractor shall promptly provide the City with copies of its data required for the City to meet its necessary disclosure obligations.
- 3.5. **Mandatory Disclosures:** In addition to the requirements set forth herein, the Contractor shall provide the City with a copy of any disclosure the Contractor is required to file with any regulatory body as a result of a Security Breach or other incident that requires the Contractor to make such a disclosure, including but not limited to, required disclosures mandated by the Securities and Exchange Commission. If the contents of any such disclosure is protected by law, the Contractor shall instead provide the City with prompt notice that it was required to make such a disclosure along with the name of the regulatory body requiring the Contractor to make such a disclosure.
- 3.6. **Data Retention, Transfer, Holds, and Destruction:** Using appropriate and reliable storage media, the Contractor shall regularly backup data used in connection with this Agreement and retain such backup copies as necessary to meet its obligations hereunder. All City Data shall be encrypted in transmission, including by web interface, and in storage by an agreed upon National Institute of Standards and Technology (“NIST”) approved strong encryption method and standard. Upon the expiration or termination of this Agreement, the Contractor shall, as directed by the City, provide a copy of all City Data to the City. Contractor will retain metadata as required by law. The Contractor shall not interrupt or obstruct the City’s ability to access and retrieve City Data stored by the Contractor. Unless otherwise required by law or regulation, when paper or electronic documents are no longer needed, the Contractor shall destroy or arrange for the destruction of such documents within its custody or control that contain City Data by shredding, erasing, or otherwise modifying the City Data in the paper or electronic documents to make it unreadable or indecipherable. The Contractor’s obligations set forth in this Subsection, without limitation, apply likewise to the Contractor’s successors, including without limitation any trustee in bankruptcy.
- 3.7. **Software and Computing Systems:** At its reasonable discretion, the City may prohibit the Contractor from the use of certain software programs, databases, and computing systems with known vulnerabilities to collect, use, process, or store, City Data received under this Agreement. The Contractor shall fully comply with all requirements and conditions, if any, associated with

the use of software programs, databases, and computing systems as reasonably directed by the City. The Contractor shall not use funds paid by the City for the acquisition, operation, or maintenance of software in violation of any copyright laws or licensing restrictions. The Contractor shall maintain commercially reasonable network security that, at a minimum, includes network firewalls, intrusion detection/prevention, and enhancements or updates consistent with evolving industry standards. The Contractor shall use industry-standard and up-to-date security tools, technologies and procedures including, but not limited to, anti-virus and anti-malware protections. The Contractor shall ensure that any underlying or integrated software employed under this Agreement is updated on a regular basis and does not pose a security threat. Upon request, the Contractor shall provide a software bill of materials (“SBOM”) annually or upon major changes to the solution(s) provided to the City under this Agreement. The Contractor shall provide a complete SBOM for the supported life of the solution(s). The Contractor shall monitor for security vulnerabilities in applicable software components and use a risk-based approach to mitigate any vulnerabilities.

- 3.8. Background Checks:** The Contractor shall ensure that, prior to being granted access to City Data, the Contractor’s agents, employees, Subcontractors, volunteers, or assigns who perform work under this Agreement have all undergone and passed all necessary criminal background screenings, have successfully completed annual instruction of a nature sufficient to enable them to effectively comply with all data protection provisions of this Agreement and applicable law, and possess all qualifications appropriate to the nature of the employees’ duties and the sensitivity of the data. If the Contractor has access to federal tax information (“FTI”) under this Agreement, the Contractor shall comply with the background check requirements of IRS Publication 1075.
- 3.9. Subcontractors:** If the Contractor engages a Subcontractor under this Agreement, the Contractor shall ensure its Subcontractors are subject to data protection terms that provide at least the same level of data protection as in this Agreement and to the extent appropriate to the nature of the Work provided. The Contractor shall monitor the compliance with such obligations and remain responsible for its Subcontractor’s compliance with the obligations of this Agreement and for any of its Subcontractors acts or omissions that cause the Contractor to breach any of its obligations under this Agreement. Unless the Contractor provides its own security protection for the information it discloses to a third party, the Contractor shall require the third party to implement and maintain reasonable security procedures and practices that are appropriate to the nature of the City Data disclosed and that are reasonably designed to protect it from unauthorized access, use, modification, disclosure, or destruction. Any term or condition within this Agreement relating to the protection and confidentiality of any disclosed data shall apply equally to both the Contractor and any of its Subcontractors, agents, assigns, employees, or volunteers. Upon request, the Contractor shall provide the City copies of its record retention, data privacy, and information security policies. The Contractor shall ensure all Subcontractors sign, or have signed, agreements containing nondisclosure provisions at least as protective as those in this Agreement, and that the nondisclosure provisions are in force so long as the Subcontractor has access to any data disclosed

under this Agreement. Upon request, the Contractor shall provide copies of those signed nondisclosure agreements to the City.

- 3.10. Request for Additional Protections and Survival:** In addition to the terms contained herein, the City may reasonably request that the Contractor protect the confidentiality of certain City Data to ensure compliance with applicable law and any changes thereto. Unless a request for additional protections is mandated by a change in law, the Contractor may reasonably decline the City's request to provide additional protections. If such a request requires the Contractor to take steps beyond those contained herein, the Contractor shall notify the City with the anticipated cost of compliance, and the City may thereafter, in its sole discretion, direct the Contractor to comply with the request at the City's expense; provided, however, that any increase in costs that would increase the Maximum Contract Amount must first be memorialized in a written amendment complying with City procedures. Obligations contained in this Agreement relating to the protection and confidentiality of any disclosed data shall survive termination of this Agreement, and the Contractor shall continue to safeguard all data for so long as the data remains confidential or protected and in the Contractor's possession or control.

4. DISASTER RECOVERY AND CONTINUITY

- 4.1.** The Contractor shall maintain a continuous and uninterrupted business continuity and disaster recovery program with respect to the Work provided under this Agreement. The program shall be designed, in the event of a significant business disruption affecting the Contractor, to provide the necessary and sufficient capabilities, processes, and procedures to enable the Contractor to resume and continue to perform its duties and obligations under this Agreement without undue delay or disruption. In the event of equipment failures, the Contractor shall, at no additional expense to the City, take reasonable steps to minimize service interruptions, including using any back-up facilities where appropriate. Upon request, the Contractor shall provide the City with a copy of its disaster recovery plan and procedures.
- 4.2.** Prior to the Effective Date of this Agreement, the Contractor shall, at its own expense, conduct or have conducted the following, and thereafter, the Contractor will, at its own expense, conduct or have conducted the following at least once per year:
- 4.2.1.** A test of the operability, sufficiency, and completeness of business continuity and disaster recovery program's capabilities, processes, and procedures that are necessary to resume and continue to perform its duties and obligations under this Agreement.
- 4.2.2.** Based upon the results and subsequent recommendations of the testing above, the Contractor will, within thirty (30) calendar days of receipt of such results and recommendations, promptly modify its capabilities, processes, and procedures to meet its obligations under this Agreement and provide City with written evidence of remediation.
- 4.2.3.** Upon request, the Contractor shall provide the City with report summaries or other documentation resulting from above testing of any business continuity and disaster recovery procedures regarding the Services provided under this Agreement.

- 4.3. The Contractor represents that it is capable, willing, and able to provide the necessary and sufficient business continuity and disaster recovery capabilities and functions that are appropriate for it to provide services under this Agreement.

5. **DELIVERY AND ACCEPTANCE**

5.1. **Acceptance & Rejection**: Deliverables will be considered accepted (“Acceptance”) only when the City provides the Contractor affirmative written notice of acceptance that such Deliverable has been accepted by the City. Such communication shall be provided within a reasonable time from the delivery of the Deliverable and shall not be unreasonably delayed or withheld. Acceptance by the City shall be final, except in cases of Contractor’s failure to conduct proper quality assurance, latent defects that could not reasonably have been detected upon delivery, or the Contractor’s gross negligence or willful misconduct. The City may reject a Deliverable if it materially deviates from its specifications and requirements listed in this Agreement or its Exhibits by written notice setting forth the nature of such deviation. In the event of such rejection, the Contractor shall correct the deviation, at its sole expense, and redeliver the Deliverable within fifteen (15) days. After redelivery, the Parties shall again follow the acceptance procedures set forth herein. If any Deliverable does not perform to the City’s satisfaction, the City reserves the right to repudiate acceptance. If the City ultimately rejects a Deliverable, or repudiates acceptance of it, the Contractor will refund to the City all fees paid, if any, by the City with respect to any rejected Deliverable. Acceptance shall not relieve the Contractor from its responsibility under any representation or warranty contained in this Agreement, and payment of an invoice prior to Acceptance does not grant a waiver of any representation or warranty made by the Contractor.

5.2. **Quality Assurance**: The Contractor shall provide and maintain a quality assurance system acceptable to the City for Deliverables under this Agreement and shall provide to the City only such Deliverables that have been inspected and found to conform to the specifications identified in this Agreement and any applicable solicitation, bid, offer, or proposal from which this Agreement results. The Contractor’s delivery of any Deliverables to the City shall constitute certification that any Deliverables have been determined to conform to the applicable specifications, and the Contractor shall make records of such quality assurance available to the City upon request.

6. **WARRANTIES AND REPRESENTATIONS**

6.1. Notwithstanding the acceptance of any Work, or the payment of any invoice for such Work, the Contractor warrants that any Work provided by the Contractor under this Agreement shall be free from material defects and shall function as intended and in material accordance with the applicable Specifications. The Contractor warrants that any Work, and any media used to distribute it, shall be, at the time of delivery, free from any harmful or malicious code, including without limitation viruses, malware, spyware, ransomware, or other similar function or technological means designed to disrupt, interfere with, or damage the normal operation of the Work and the use of City resources and systems. The Contractor’s warranties under this Section shall apply to any defects or material nonconformities discovered within 180 days following delivery of any Work.

- 6.2.** Upon notice of any defect or material nonconformity, the Contractor shall submit to the City in writing within 10 business days of the notice one or more recommendations for corrective action with sufficient documentation for the City to ascertain the feasibility, risks, and impacts of each recommendation. The City's remedy for such defect or material non-conformity shall be:
- 6.2.1.** The Contractor shall re-perform, repair, or replace such Work in accordance with any recommendation chosen by the City. The Contractor shall deliver, at no additional cost to the City, all documentation required under this Agreement as applicable to the corrected Work or Deliverable; or
- 6.2.2.** The Contractor shall refund to the City all amounts paid for such Work, as well as pay to the City any additional amounts reasonably necessary for the City to procure alternative goods or services of substantially equivalent capability, function, and performance.
- 6.3.** Any Work delivered to the City as a remedy under this Section shall be subject to the same quality assurance, acceptance, and warranty requirements as the original Work. The duration of the warranty for any replacement or corrected Work shall run from the date of the corrected or replacement Work.
- 6.4. Customization Services:** The Contractor warrants that it will perform all customization services, if any, in a professional and workmanlike manner. In case of breach of the warranty of the preceding sentence, the Contractor, at its own expense, shall promptly re-perform the customization services in question or provide a full refund for all nonconforming customization services.
- 6.5. Third-Party Warranties and Indemnities:** The Contractor will assign to the City all third-party warranties and indemnities that the Contractor receives in connection with any Work or Deliverables provided to the City. To the extent that the Contractor is not permitted to assign any warranties or indemnities through to the City, the Contractor agrees to specifically identify and enforce those warranties and indemnities on behalf of the City to the extent the Contractor is permitted to do so under the terms of the applicable third-party agreements.
- 6.6. Intellectual Property Rights in the Software:** The Contractor warrants that it is the owner of all Deliverables, and of each and every component thereof, or the recipient of a valid license thereto, and that it has and will maintain the full power and authority to grant the intellectual property rights to the Deliverables in this Agreement without the further consent of any third party and without conditions or requirements not set forth in this Agreement. In the event of a breach of the warranty in this Section, the Contractor, at its own expense, shall promptly take the following actions: (i) secure for the City the right to continue using the Deliverable as intended; (ii) replace or modify the Deliverable to make it non-infringing, provided such modification or replacement will not materially degrade any functionality as stated in this Agreement; or (iii) refund 100% of the fee paid for the Deliverable for every month remaining in the Term, in which case the Contractor may terminate any or all of the City's licenses to the infringing Deliverable granted in this Agreement and require return or destruction of copies thereof. The Contractor also warrants that there are no pending or threatened lawsuits, claims, disputes, or actions: (i) alleging that any of the Work or Deliverables infringes, violates, or misappropriates any third-party rights; or (ii)

adversely affecting any Deliverables or Services, or the Contractor's ability to perform its obligations hereunder.

- 6.7. Disabling Code:** The Work will contain no malicious or disabling code that is intended to damage, destroy, or destructively alter software, hardware, systems, or data. The Contractor represents, warrants and agrees that the City will not receive from the Contractor any virus, worm, trap door, back door, timer, clock, counter or other limiting routine, instruction or design, or other malicious, illicit or similar unrequested code, including surveillance software or routines which may, or is designed to, permit access by any person, or on its own, to erase, or otherwise harm or modify any City system, resources, or data (a "Disabling Code"). In the event a Disabling Code is identified, the Contractor shall take all steps necessary, at no additional cost to the City, to: (i) restore and/or reconstruct all data lost by the City as a result of a Disabling Code; (ii) furnish to City a corrected version of the Work or Deliverables without the presence of a Disabling Code; and, (iii) as needed, re-implement the Work or Deliverable at no additional cost to the City. This warranty shall remain in full force and effect during the Term.

7. PAYMENT CARD INDUSTRY DATA SECURITY STANDARD COMPLIANCE

- 7.1.** If the Contractor is directly involved in the processing, storage, or transmission of cardholder data on behalf of the City as part of this Agreement, this Section shall apply. Any contractor who provides or has access to software, systems, hardware, or devices which process and/or interact with payment card information or payment cardholder data must be compliant with the current version of the Payment Card Industry Data Security Standard (PCI DSS).
- 7.2.** The Contractor covenants and agrees to comply with Visa's Cardholder Information Security Program (CISP), MasterCard's Site Data Protection Rules (SDP), and with all other credit card association or National Automated Clearing House Association (NACHA) rules or rules of member organizations ("Association"), and further covenants and agrees to maintain compliance with the PCI DSS, SDP, and (where applicable) the Payment Application Data Security Standard (PA-DSS) (collectively, the "Security Guidelines"). The Contractor represents and warrants that all of the hardware and software components utilized for the City or used under this Agreement is now and will be PCI DSS compliant during the term of this Agreement. All service providers that the Contractor uses under this Agreement must be recognized by Visa as PCI DSS compliant. The Contractor further agrees to exercise reasonable due diligence to ensure that all of its service providers (as defined by the PCI Security Council), agents, business partners, contractors, Subcontractors, and any third party who may have access to credit card information under this Agreement maintain compliance with the Security Guidelines and comply in full with the terms and conditions set out in this Section. The Contractor further certifies that the equipment, as described herein, will be deployed in a manner that meets or exceeds the PA DSS and/or PCI certification and will be deployed on a network that meets or exceeds PCI standards. The Contractor shall demonstrate its compliance with PCI DSS by annually providing the City an executed Attestation of Compliance (AOC). The Contractor must provide verification to the City, prior to start up and ongoing annually during the term of this Agreement, that all modules of the Contractor's system(s) that interface with or utilize credit card information in any manner or form

of collection are PCI DSS compliant. If the Contractor is a service provider involved in the processing, storage or transmission of cardholder data or sensitive authentication data (collectively “Data Handling”) on behalf of the City that would result in Data Handling being included in the City's PCI scope through connected software or components, then the Contractor must provide a PCI Responsibility Matrix (“Matrix”) to be attached to this Agreement as an exhibit. The Matrix must identify where responsibility resides for each PCI control requirement, whether it be with the Contractor, the City or shared by both. Any PCI control requirements that do not apply should be indicated along with any pertinent notes.

- 7.3. The Contractor shall not retain or store CAV2/CVC2/CVV2/CID or such data prohibited by PCI DSS subsequent to authorization of a credit card transaction, shall prohibit disclosure of any and all cardholder information, and in the event of a compromise of credit card information of any kind, the Contractor shall notify the City in writing consistent with the Security Breach response notification requirements of this Agreement, and shall provide, at the Contractor’s sole expense, all necessary and appropriate notification to parties and persons affected by such disclosure and compromise.
- 7.4. If any Association requires an audit of the Contractor or any of the Contractor’s Service Providers, agents, business partners, contractors, or Subcontractors due to a data security compromise event related to this Agreement, the Contractor agrees to cooperate with such audit. If as a result of an audit of the City it is determined that any loss of information is attributable to the Contractor, the Contractor shall pay the City’s reasonable costs relating to such audit, including attorney’s fees. No review, approval, or audit by the City shall relieve the Contractor from liability under this Section or under other provisions of this Agreement.
- 7.5. The Contractor is solely responsible for its PCI DSS compliance. The Contractor shall ensure that all PCI DSS vendors comply with PCI DSS standards: (i) in providing Services or Deliverables to the City under this Agreement; (ii) in storing, processing, or transmitting PCI data; and (iii) in engaging in any other activities for any purpose relating to this Agreement. As between the Contractor and the City, the Contractor shall be responsible for a PCI DSS vendor's non-compliance with PCI DSS.
- 7.6. In addition to all other defense and indemnity obligations undertaken by the Contractor under this Agreement, the Contractor, to the extent that its performance of this Agreement includes the allowance or utilization by members of the public of credit cards to pay monetary obligations to the City or the Contractor, or includes the utilization, processing, transmittal and/or storage of credit card data by the Contractor, shall defend, release, indemnify and save and hold harmless the City against any and all fines, penalties, assessments, costs, damages or other financial obligations, however denominated, assessed against the City and/or the Contractor by credit card company(s), financial institution(s) or by the National Automated Clearing House Association (NACHA) or successor or related entity, including but not limited to, any credit card company fines, regardless of whether considered to be consequential, special, incidental or punitive damages, costs of notifying parties and persons affected by credit card information disclosure, the cost of replacing active credit cards, and any losses associated with fraudulent transaction(s)

occurring after a security breach or loss of information with respect to credit card information, and shall defend, release, indemnify, and save and hold harmless the City from any and all claims, demands, suits, actions, liabilities, causes of action or legal or equitable proceedings of any kind or nature, of or by anyone whomsoever, in any way affected by such credit card data or utilizing a credit card in the performance by the Contractor of this Agreement. In furtherance of this, the Contractor covenants to defend and indemnify the City and the Contractor shall maintain compliance with PCI DSS and with all other requirements and obligations related to credit card data or utilization set out in this Agreement.

8. LICENSE OR USE AUDIT RIGHTS

- 8.1.** To the extent that the Contractor, through this Agreement or otherwise as related to the subject matter of this Agreement, has granted to the City any license or otherwise limited permission to use any of the Contractor's intellectual property, the terms of this Section shall apply.
- 8.2.** The Contractor shall have the right, at any time during and throughout the Term, but not more than once per year, to request via written notice in accordance with the notice provisions of this Agreement that the City audit its use of and certify as to its compliance with any applicable license or use restrictions and limitations contained in this Agreement (an "Audit Request"). The Audit Request shall specify the period to be covered by the audit, which shall not include any time covered by a previous audit. The City shall complete the audit and provide certification of its compliance to the Contractor ("Audit Certification") within a reasonable amount of time following the City's receipt of the Audit Request.
- 8.3.** If upon receipt of the City's Audit Certification, the Parties reasonably determine that: (i) the City's use of licenses, use of software, use of programs, or any other use during the audit period exceeded the use restrictions and limitations contained in this Agreement ("Overuse"), and (ii) the City would have been or is then required to purchase additional maintenance and/or services ("Maintenance"), the Contractor shall provide written notice to the City in accordance with the notice provisions of this Agreement identifying any Overuse or required Maintenance and request that the City bring its use into compliance with such use restrictions and limitations.

REMAINDER OF PAGE INTENTIONALLY LEFT BLANK



Exhibit G - CERTIFICATE OF LIABILITY INSURANCE

 DATE(MM/DD/YYYY)
02/12/2025

THIS CERTIFICATE IS ISSUED AS A MATTER OF INFORMATION ONLY AND CONFERS NO RIGHTS UPON THE CERTIFICATE HOLDER. THIS CERTIFICATE DOES NOT AFFIRMATIVELY OR NEGATIVELY AMEND, EXTEND OR ALTER THE COVERAGE AFFORDED BY THE POLICIES BELOW. THIS CERTIFICATE OF INSURANCE DOES NOT CONSTITUTE A CONTRACT BETWEEN THE ISSUING INSURER(S), AUTHORIZED REPRESENTATIVE OR PRODUCER, AND THE CERTIFICATE HOLDER.

IMPORTANT: If the certificate holder is an ADDITIONAL INSURED, the policy(ies) must have ADDITIONAL INSURED provisions or be endorsed. If SUBROGATION IS WAIVED, subject to the terms and conditions of the policy, certain policies may require an endorsement. A statement on this certificate does not confer rights to the certificate holder in lieu of such endorsement(s).

PRODUCER Aon Risk Insurance Services West, Inc. Denver CO Office 200 Clayton Street, Suite 800 Denver CO 80206 USA	CONTACT NAME: PHONE (A/C. No. Ext): (866) 283-7122 FAX (A/C. No.): (800) 363-0105 E-MAIL ADDRESS: 														
INSURED Securus Technologies, LLC 4000 International Parkway Carrollton TX 75007 USA	<table border="1"> <thead> <tr> <th data-bbox="795 514 1380 535">INSURER(S) AFFORDING COVERAGE</th> <th data-bbox="1380 514 1520 535">NAIC #</th> </tr> </thead> <tbody> <tr> <td data-bbox="795 535 1380 556">INSURER A: Lloyd's Syndicate No. 2623</td> <td data-bbox="1380 535 1520 556">AA1128623</td> </tr> <tr> <td data-bbox="795 556 1380 577">INSURER B: Valley Forge Insurance Co</td> <td data-bbox="1380 556 1520 577">20508</td> </tr> <tr> <td data-bbox="795 577 1380 598">INSURER C: National Fire Ins. Co. of Hartford</td> <td data-bbox="1380 577 1520 598">20478</td> </tr> <tr> <td data-bbox="795 598 1380 619">INSURER D: The Continental Insurance Company</td> <td data-bbox="1380 598 1520 619">35289</td> </tr> <tr> <td data-bbox="795 619 1380 640">INSURER E:</td> <td data-bbox="1380 619 1520 640"></td> </tr> <tr> <td data-bbox="795 640 1380 661">INSURER F:</td> <td data-bbox="1380 640 1520 661"></td> </tr> </tbody> </table>	INSURER(S) AFFORDING COVERAGE	NAIC #	INSURER A: Lloyd's Syndicate No. 2623	AA1128623	INSURER B: Valley Forge Insurance Co	20508	INSURER C: National Fire Ins. Co. of Hartford	20478	INSURER D: The Continental Insurance Company	35289	INSURER E:		INSURER F:	
INSURER(S) AFFORDING COVERAGE	NAIC #														
INSURER A: Lloyd's Syndicate No. 2623	AA1128623														
INSURER B: Valley Forge Insurance Co	20508														
INSURER C: National Fire Ins. Co. of Hartford	20478														
INSURER D: The Continental Insurance Company	35289														
INSURER E:															
INSURER F:															

COVERAGES **CERTIFICATE NUMBER:** 570110851648 **REVISION NUMBER:**

THIS IS TO CERTIFY THAT THE POLICIES OF INSURANCE LISTED BELOW HAVE BEEN ISSUED TO THE INSURED NAMED ABOVE FOR THE POLICY PERIOD INDICATED. NOTWITHSTANDING ANY REQUIREMENT, TERM OR CONDITION OF ANY CONTRACT OR OTHER DOCUMENT WITH RESPECT TO WHICH THIS CERTIFICATE MAY BE ISSUED OR MAY PERTAIN, THE INSURANCE AFFORDED BY THE POLICIES DESCRIBED HEREIN IS SUBJECT TO ALL THE TERMS.

INSR LTR	TYPE OF INSURANCE	ADDL INSD	SUBR WVD	POLICY NUMBER	POLICY EFF (MM/DD/YYYY)	POLICY EXP (MM/DD/YYYY)	Limits shown as requested LIMITS	
B	<input checked="" type="checkbox"/> COMMERCIAL GENERAL LIABILITY <input type="checkbox"/> CLAIMS-MADE <input checked="" type="checkbox"/> OCCUR GEN'L AGGREGATE LIMIT APPLIES PER: <input checked="" type="checkbox"/> POLICY <input type="checkbox"/> PRO-JECT <input type="checkbox"/> LOC OTHER:			7094249270	09/30/2024	09/30/2025	EACH OCCURRENCE \$1,000,000 DAMAGE TO RENTED PREMISES (Ea occurrence) \$100,000 MED EXP (Any one person) \$15,000 PERSONAL & ADV INJURY \$1,000,000 GENERAL AGGREGATE \$2,000,000 PRODUCTS - COMP/OP AGG \$2,000,000	
C	AUTOMOBILE LIABILITY <input checked="" type="checkbox"/> ANY AUTO <input type="checkbox"/> OWNED AUTOS ONLY <input type="checkbox"/> SCHEDULED AUTOS <input type="checkbox"/> HIRED AUTOS ONLY <input type="checkbox"/> NON-OWNED AUTOS ONLY			7094249267	09/30/2024	09/30/2025	COMBINED SINGLE LIMIT (Ea accident) \$1,000,000 BODILY INJURY (Per person) BODILY INJURY (Per accident) PROPERTY DAMAGE (Per accident)	
D	<input checked="" type="checkbox"/> UMBRELLA LIAB <input checked="" type="checkbox"/> OCCUR <input type="checkbox"/> EXCESS LIAB <input type="checkbox"/> CLAIMS-MADE DED <input checked="" type="checkbox"/> RETENTION \$10,000			CUE7094249253	09/30/2024	09/30/2025	EACH OCCURRENCE \$10,000,000 AGGREGATE \$10,000,000	
B	WORKERS COMPENSATION AND EMPLOYERS' LIABILITY ANY PROPRIETOR / PARTNER / EXECUTIVE OFFICER/MEMBER (Mandatory in NH) If yes, describe under DESCRIPTION OF OPERATIONS below	Y/N N	N/A	794249284	09/30/2024	09/30/2025	<input checked="" type="checkbox"/> PER STATUTE <input type="checkbox"/> OTHER E.L. EACH ACCIDENT \$1,000,000 E.L. DISEASE-EA EMPLOYEE \$1,000,000 E.L. DISEASE-POLICY LIMIT \$1,000,000	
A	Cyber Liability			W1C7D5230801 Cyber/Errors & Omissions	11/29/2023	03/31/2025	Aggregate \$5,000,000	

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required)

Professional E&O is included on the Cyber Liability policy. City and County of Denver its elected and appointed officials, employees and volunteers are included as Additional Insured in accordance with the policy provisions of the General Liability, Automobile Liability and Umbrella Liability policies. General Liability policy evidenced herein is Primary and Non-Contributory to other insurance available to an Additional Insured, but only in accordance with the policy's provisions. A waiver of Subrogation is granted in favor of Additional Insureds in accordance with the policy provisions of the General Liability, Automobile Liability, Umbrella Liability, Cyber Liability and workers Compensation policies. Umbrella Liability policy follows Form. TECHS-202577792-00

CERTIFICATE HOLDER

City and County of Denver
 Manager of Safety
 1331 Cherokee Street
 Room 302
 Denver CO 80202 USA

CANCELLATION

SHOULD ANY OF THE ABOVE DESCRIBED POLICIES BE CANCELLED BEFORE THE EXPIRATION DATE THEREOF, NOTICE WILL BE DELIVERED IN ACCORDANCE WITH THE POLICY PROVISIONS.

AUTHORIZED REPRESENTATIVE

Aon Risk Insurance Services West, Inc.

Holder Identifier :

570110851648

Certificate No :