

## **MASTER SERVICES 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, INC.**, a Delaware corporation, registered to do business in Colorado, whose address is 14651 Dallas Parkway, Suite 600, Dallas, TX 78254 ("Contractor"), jointly "the parties."

IT IS HEREBY AGREED BETWEEN THE PARTIES AS FOLLOWS:

**1. SOFTWARE LICENSE, SUPPORT, HARDWARE AND MAINTENANCE TO BE PROVIDED AND SERVICES TO BE PERFORMED:**

**A.** Contractor, under the general direction of, and in coordination with, the City's Manager of Safety or other designated supervisory personnel (the "Manager") agrees to provide the software (the "Software") including ConnectUs Inmate Service Platform (separately described in Schedule 1) and hardware ("Hardware"), perform the technology related services (the "Statement of Work" or "SOW") and provide the software support and maintenance services described on attached **Exhibits A, D and E**. All of the preceding deliverables will comply with the City's Enterprise Architecture Technology Standards, Attachment 1 and conform to the requirements of Attachments 2 and 3.

**B.** As the Manager directs, the Contractor shall diligently undertake, perform, and complete all of the services and produce all the deliverables set forth on to the City's satisfaction.

**C.** The Contractor is ready, willing, and able to provide the services required by this Agreement.

**D.** The Contractor shall faithfully perform the 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 the Agreement and in accordance with the terms of the Agreement.

**2. GRANT OF LICENSE; RESTRICTIONS:**

**A.** Contractor hereby grants to City a perpetual, irrevocable, non-exclusive right and license to: (a) install, display, perform, and use the Software; and (b) use all intellectual property rights necessary to use the Software as authorized in subparagraph (a).

**B.** Title to and ownership of the Software will remain with Contractor. City will not reverse engineer or reverse compile any part of the Software without Contractor's prior written consent. City will not remove, obscure or deface any proprietary notice or legend contained in the Software or documentation without Contractor's prior written consent.

3. **DELIVERY AND ACCEPTANCE:**

A. Contractor shall deliver the Software and Hardware and perform the services in accordance with the SOW, Video Visitation Schedule and Attachments 1, 2 and 3.

B. Upon installation and configuration of the Software and Hardware, the City will test and evaluate same to ensure that it conforms to the specifications outlined in the SOW and its intended purposes. If the Software and Hardware does not conform, the City will so notify Contractor in writing within sixty (60) days. Contractor will, at its expense, repair or replace the nonconforming product within fifteen (15) days after receipt of the City's notice of deficiency. The foregoing procedure will be repeated until the City accepts or finally rejects the product, in whole or part, in its reasonable discretion. In the event that the Software contains a defect or nonconformity not apparent on examination, the City reserves the right to repudiate acceptance. In the event that the City finally rejects the Software, or repudiates acceptance of it, Contractor will refund to the City all fees paid, if any, by the City with respect to the rejected product.

C. If the City is not satisfied with the Contractor's performance of the services described in the SOW, the City will so notify Contractor in writing within thirty (30) days after Contractor's performance thereof. Contractor will, at its own expense, re-perform the service within thirty (30) days after receipt of City's notice of deficiency. Notwithstanding the foregoing, the 30 day cure period will be extended to 90 days if the unsatisfactory performance is not reasonably susceptible to cure within such 30 day period. The foregoing procedure will be repeated until City accepts or finally rejects the service in its reasonable discretion. In the event that City finally rejects any service, Contractor will refund to City all fees paid by City with respect to such service.

E. The Contractor shall warrant the operation of the Hardware for a period of one year from the date of delivery to the City.

4. **TERM:** The term of the Agreement is from June 1, 2017 through December 31, 2021.

5. **COMPENSATION AND PAYMENT:**

A. **Fee:** The fee for the Software, Hardware and services is described in Exhibits A and D (the "Fee"). The Fee shall be paid pursuant to the City's Prompt Payment Ordinance and in accordance with the Payment Milestones in the SOW.

B. **Reimbursement Expenses:** The fees specified above include all expenses, and no other expenses shall be separately reimbursed hereunder.

C. **Invoicing:** Contractor must submit an invoice which shall include the City contract number, clear identification of the deliverable that has been completed, and other information reasonably requested by the City. Payment on all uncontested amounts shall be made in accordance with the City's Prompt Payment Ordinance. Payment for the Video

Visitation will be made in two phases. The Phase I payment of \$516,533 for Video Visitation at the Denver County Jail will be due within 30 days of successful installation. Phase II payment and installation are contingent upon budget approval. If approved, the Phase II payment of \$895,467 for Video Visitation at the Downtown Detention Center will be due within 30 days of successful installation.

**D. Maximum Contract Liability:**

(i) Notwithstanding any other provision of the Agreement, the City's maximum payment obligation will not exceed **ONE MILLION FOUR HUNDRED AND TWELVE THOUSAND DOLLARS (\$1,412,000.00)** (the "Maximum Contract Amount"). The City is not obligated to execute an Agreement or any amendments for any further services, including any services performed by Contractor beyond that specifically described in **Exhibit A**. Any services performed beyond those in the Exhibits are performed at Contractor's risk and without authorization under the Agreement.

(ii) 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 the Agreement. The City does not by the Agreement irrevocably pledge present cash reserves for payment or performance in future fiscal years. The Agreement does not and is not intended to create a multiple-fiscal year direct or indirect debt or financial obligation of the City.

**6. 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.

**7. TERMINATION:**

**A.** The City has the right to terminate the Agreement with cause upon 30 days written notice and without cause upon 90 days prior written notice to the Contractor. However, nothing gives the Contractor the right to perform services under the Agreement beyond the time when its services become unsatisfactory to the Manager.

**B.** Notwithstanding the preceding paragraph, the City may terminate the 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, kick backs, collusive bidding, bid-rigging, antitrust, fraud, undue influence, theft, racketeering, extortion or any offense of a similar nature in connection with Contractor's business. Termination for the reasons stated in this paragraph is effective upon receipt of notice.

8. **EXAMINATION OF RECORDS:** 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 any pertinent books, documents, papers and records of the Contractor, involving transactions related to the Agreement until the latter of three (3) years after the final payment under the Agreement or expiration of the applicable statute of limitations.

9. **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 the Agreement shall be deemed or taken to be a waiver of any other breach.

10. **INSURANCE:**

A. **General Conditions:** 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. Contractor shall keep the required insurance coverage in force at all times during the term of the Agreement, or any extension thereof, during any warranty period, and for three (3) years after termination of the Agreement. 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 contain a valid provision or endorsement requiring notification to the City in the event any of the required policies is 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, 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. If any policy is in excess of a deductible or self-insured retention, the City must be notified by the Contractor. 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.

B. **Proof of Insurance:** Contractor shall provide a copy of this Agreement to its insurance agent or broker. Contractor may not commence services or work relating to the Agreement prior to placement of coverages required under this Agreement. Contractor certifies that the certificate of insurance attached as Exhibit B, preferably an ACORD certificate, complies with all insurance requirements of this Agreement. The City requests that the City's

contract number be referenced on the Certificate. 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 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.

C. **Additional Insureds:** For Commercial General Liability, Auto Liability and Excess Liability/Umbrella (if required), 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.

D. **Waiver of Subrogation:** For all coverages required under this Agreement, Contractor's insurer shall waive subrogation rights against the City.

E. **Subcontractors and Subconsultants:** All subcontractors and subconsultants (including independent contractors, suppliers or other entities providing goods or services required by this Agreement) shall be subject to all of the requirements herein and shall procure and maintain the same coverages required of the Contractor. Contractor shall include all such subcontractors as additional insured under its policies (with the exception of Workers' Compensation) or shall ensure that all such subcontractors and subconsultants maintain the required coverages. Contractor agrees to provide proof of insurance for all such subcontractors and subconsultants upon request by the City.

F. **Workers' Compensation/Employer's Liability Insurance:** 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. Contractor expressly represents to the City, as a material representation upon which the City is relying in entering into this Agreement, that none of the Contractor's officers or employees who may be eligible under any statute or law to reject Workers' Compensation Insurance shall effect such rejection during any part of the term of this Agreement, and that any such rejections previously effected, have been revoked as of the date Contractor executes this Agreement.

G. **Commercial General Liability:** Contractor shall maintain a Commercial General Liability insurance policy with limits of \$1,000,000 for each occurrence, \$1,000,000 for each personal and advertising injury claim, \$2,000,000 products and completed operations aggregate, and \$2,000,000 policy aggregate.

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

I. **Technology Errors & Omissions with Cyber-Liability:** Contractor shall maintain Technology Errors and Omissions insurance including cyber liability, network security,

privacy liability and product failure coverage with limits of \$1,000,000 per occurrence and \$1,000,000 policy aggregate.

**J. Additional Provisions:**

- (a) For Commercial General Liability, the policy must provide the following:
  - (i) That this Agreement is an Insured Contract under the policy;
  - (ii) Defense costs are outside the limits of liability;
  - (iii) A severability of interests or separation of insureds provision (no insured vs. insured exclusion); and
  - (iv) A provision that coverage is primary and non-contributory with other coverage or self-insurance maintained by the City.
  
- (b) For claims-made coverage:
  - (i) The retroactive date must be on or before the contract date or the first date when any goods or services were provided to the City, whichever is earlier.
  
  - (ii) Contractor shall advise the City in the event any general aggregate or other aggregate limits are reduced below the required per occurrence limits. At their own expense, and where such general aggregate or other aggregate limits have been reduced below the required per occurrence limit, the Contractor will procure such per occurrence limits and furnish a new certificate of insurance showing such coverage is in force.

**11. REPRESENTATION AND WARRANTY:** Contractor represents and warrants that:

**A.** Contractor agrees to repair and maintain the System and Software in good operating condition (ordinary wear and tear excepted), including, without limitation, furnishing all parts and labor and that all such maintenance will be conducted in accordance with the Service Level Agreements;

**B.** all services will be performed by qualified personnel in a professional and workmanlike manner, consistent with industry standards;

**C.** all services will conform to applicable specifications and the Exhibits attached hereto;

**D.** 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 the software and services free and clear from any and all liens, adverse claims, encumbrances and interests of any third party;

E. there are no pending or threatened lawsuits, claims, disputes or actions: (i) alleging that any software or service infringes, violates or misappropriates any third party rights; or (ii) adversely affecting any software, service or supplier's ability to perform its obligations hereunder;

F. the Software will not violate, infringe, or misappropriate any patent, copyright, trademark, trade secret, or other intellectual property or proprietary right of any third party;

G. the Software will contain no malicious or disabling code that is intended to damage, destroy or destructively alter software, hardware, systems or data; and

H. the media on which all Software is furnished are and will be, under normal use, free from defects in materials and workmanship.

## **12. DEFENSE AND INDEMNIFICATION:**

A. 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") by Contractor, unless such Claims have been specifically determined by the trier of fact to be the negligence or willful misconduct of the City. This indemnity shall be interpreted in the broadest possible manner to indemnify City for any acts or omissions of Contractor or its subcontractors either passive or active, irrespective of fault, including City's concurrent negligence whether active or passive, except for the negligence or willful misconduct of City. Under no circumstances will Contractor be obligated to defend or indemnify the City to the extent that the injury, loss, or damage was caused by the City's sole negligence or willful misconduct.

B. 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. 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.

C. 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 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.

D. 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.

E. This defense and indemnification obligation shall survive the expiration or termination of this Agreement.

F. Contractor will, at Contractor's expense, indemnify, defend and hold harmless the City, its officers, agents and employees from and against any loss, cost, expense or liability (including but not limited to attorney's fees and awarded damages) arising out of a claim that the Software, services, or their use by the City, infringe, violate or misappropriate a patent, copyright, trademark, trade secret or other intellectual property or proprietary right of any third party. The City will promptly notify Contractor in writing of any claim and cooperate with Contractor and its legal counsel in the defense thereof. Contractor may in its discretion (i) contest, (ii) settle, (iii) procure for the City the right to continue using the Software, or (iv) modify or replace the infringing Software so that it no longer infringes (as long as the functionality and performance are not degraded as reasonably determined by the City). The City may participate in the defense of such action at its own expense. If Contractor concludes in its reasonable judgment that none of the foregoing options are commercially reasonable, then Contractor will refund a pro rata portion (based on a 5 year straight line depreciation running from City's final acceptance of the Software) of the Software license fee(s) paid by the City under this Agreement and reimburse the City for all reasonable expenses for removal and replacement of the Software.

13. **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. (2003).

14. **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.

15. **ASSIGNMENT; SUBCONTRACTING:** Except for assignments to its affiliates or to any entity that succeeds to its business in connection with a merger or acquisition, the Contractor shall not voluntarily or involuntarily assign any of its rights or obligations, or subcontract performance obligations, under this Agreement without obtaining the Manager's prior written consent. 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 Manager has discretion whether to consent to any assignment or subcontracting, which shall not be unreasonably withheld, or to terminate the Agreement because of unauthorized assignment or subcontracting. 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 sub-consultant, subcontractor or assign.

16. **NO THIRD PARTY BENEFICIARY:** Enforcement of the terms of the Agreement and all rights of action relating to enforcement are strictly reserved to the parties. Nothing contained in the 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 the Agreement is an incidental beneficiary only.

17. **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.

18. **AGREEMENT AS COMPLETE INTEGRATION-AMENDMENTS:** The Agreement is the complete integration of all understandings between the parties as to the subject matter of the Agreement. No prior, contemporaneous or subsequent addition, deletion, or other modification has any force or effect, unless embodied in the Agreement in writing. No oral representation by any officer or employee of the City at variance with the terms of the Agreement or any written amendment to the Agreement will have any force or effect or bind the City.

19. **SEVERABILITY:** Except for the provisions of the Agreement requiring appropriation of funds and limiting the total amount payable by the City, if a court of competent jurisdiction finds any provision of the 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.

20. **CONFLICT OF INTEREST:**

A. No employee of the City shall have any personal or beneficial interest in the services or property described in the 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.

B. The Contractor shall not engage in any transaction, activity or conduct that would result in a conflict of interest under the 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 the Agreement in the event it determines a conflict exists, after it has given the Contractor written notice describing the conflict.

21. **NOTICES:** All notices required by the terms of the 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 Contractor at the address first above written, and if to the City at:

Manager of Safety,  
1331 Cherokee Street,

Room 302,  
Denver, Colorado 80202

With a copy of any such notice to:

Denver City Attorney's Office  
1437 Bannock St., Room 353  
Denver, Colorado 80202

Notices hand delivered or sent by overnight courier are effective upon delivery. Notices sent by certified mail are effective upon receipt. Notices sent by mail are effective upon deposit with the U.S. Postal Service. The parties may designate 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.

**22. DISPUTES:** All disputes between the City and Contractor arising out of or regarding the 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 Manager as defined in this Agreement.

**23. GOVERNING LAW; VENUE:** The 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 the 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 the Agreement will be in the District Court of the State of Colorado, Second Judicial District.

**24. NO DISCRIMINATION IN EMPLOYMENT:** In connection with the performance of work under the Agreement, the Contractor may not refuse to hire, discharge, promote or demote, or discriminate in matters of compensation against any person otherwise qualified, solely because of race, color, religion, national origin, gender, age, military status, sexual orientation, gender variance, marital status, or physical or mental disability. The Contractor shall insert the foregoing provision in all subcontracts.

**25. USE, POSSESSION OR SALE OF ALCOHOL OR DRUGS:** 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 Contractor from City facilities or participating in City operations.

**26. CONFIDENTIAL INFORMATION; OPEN RECORDS:**

**A. Confidential Information:** "Proprietary Data" shall mean any materials or information which may be designated or marked "Proprietary" or "Confidential", or which would not be documents subject to disclosure pursuant to the Colorado Open Records Act or

City ordinance, and either provided or made available to Contractor by the City or to the City by the Contractor. Such Proprietary Data may be in hardcopy, printed, digital or electronic format. The parties acknowledges and accepts that, in performance of all work under the terms of this Agreement, the parties may have access to Proprietary data or Confidential Information that may be owned or controlled by the other party, and that the disclosure of such Proprietary Data or Confidential Information may be damaging to the non-disclosing party or to third parties. Each party agrees that all Proprietary Data, Confidential Information or any other data or information provided or otherwise disclosed shall be held in confidence and used only in the performance of its obligations under this Agreement. Each party shall exercise the same standard of care to protect such Proprietary Data and Confidential Information as it would to protect its own proprietary or confidential data. City understands and acknowledges that Contractor, as a common carrier, is required by Section 222 of the Communications Act of 1934, as amended, 47 U.S.C. Section 222, to maintain the confidentiality of "City Proprietary Network Information", or "CPNI", which protects from disclosure consumers' sensitive personal information (including phone numbers called by a consumer; the frequency, duration, and timing of such calls; and any services purchased by the consumer). The City understands and acknowledges that such CPNI is exempt from public disclosure and agrees that it will not disclose CPNI to any third party without Contractor's prior written consent.

**B. Use and Protection of Proprietary Data or Confidential Information:**

(a) Except as expressly provided by the terms of this Agreement, the parties agree that they shall not disseminate, transmit, license, sublicense, assign, lease, release, publish, post on the internet, transfer, sell, permit access to, distribute, allow interactive rights to, or otherwise make available any data, including Proprietary Data or Confidential Information or any part thereof to any other person, party or entity in any form of media for any purpose other than performing its obligations under this Agreement. The parties further acknowledges that by providing data, Proprietary Data or Confidential Information, the disclosing party is not granting any right or license to use such data except as provided in this Agreement. Each party further agrees not to disclose or distribute to any other party, in whole or in part, the data, Proprietary Data or Confidential Information without written authorization and will immediately notify the other party if any information is requested from a third party.

(b) Each party agrees, with respect to the Proprietary Data and Confidential Information, that: (1) Each party shall not copy, recreate, reverse engineer or decompile such data, in whole or in part, unless authorized in writing; (2) Neither party shall retain copies, recreations, compilations, or decompilations, in whole or in part, of such data; and (3) Each party shall, upon the expiration or earlier termination of the Agreement, destroy (and, in writing, certify destruction) or return all such data or work products incorporating such data or information to the other.

(c) Each party shall develop, implement, maintain and use appropriate administrative, technical and physical security measures to preserve the confidentiality, integrity and availability of all electronically maintained or transmitted data received from, or on behalf of City. Both parties will ensure that all possible measures have been taken to secure the computers or any other storage devices used in connection with this Agreement. This includes industry

accepted firewalls, up-to-date anti-virus software, controlled access to the physical location of the hardware itself.

C. **Employees and Sub-Contractor:** Each party will inform its employees and officers of the obligations under this Agreement, and all requirements and obligations of Contractor under this Agreement shall survive the expiration or earlier termination of this Agreement. Neither party shall disclose Proprietary Data or Confidential Information to subcontractors unless such subcontractors are bound by non-disclosure and confidentiality provisions at least as strict as those contained in this Agreement.

D. **Disclaimer:** Notwithstanding any other provision of this Agreement, the parties are furnishing Proprietary Data and Confidential Information on an "as is" basis, without any support whatsoever, and without representation, warranty or guarantee, including but not in any manner limited to, fitness, merchantability or the accuracy and completeness of the Proprietary Data or Confidential Information.

E. **Contractor's Information:** To the extent applicable in this Agreement, the City understands and agrees that the Contractor's software and documentation including, but not limited to, source code, object code, the interface requirements document(s), acceptance test procedures, the Statement of Work, the software design, structure and organization, software screens, the user interface and the engineering know-how implemented in the software (collectively "Contractor Confidential Information") may constitute the valuable properties and trade secrets of Contractor, embodying substantial creative efforts which are secret, confidential, and not generally known by the public, and which secure to Contractor a competitive advantage. The City agrees during the term of this Agreement and any license granted hereunder, and thereafter, to hold the Contractor Confidential Information including any copies thereof and any documentation related thereto, in strict confidence and to not permit any person or entity to obtain access to it except as required for the City's exercise of the license rights granted hereunder, and except as required by the parties understand that all the material provided or produced under this Agreement may be subject to the Colorado Open Records Act., § 24-72-201, et seq., C.R.S. In the event of a request to the City for disclosure of such information, the City shall advise Contractor of such request in order to give Contractor the opportunity to object to the disclosure of any of its Contractor Confidential Information and take necessary legal recourse. In the event of the filing of a lawsuit to compel such disclosure, the City will tender all such material to the court for judicial determination of the issue of disclosure and Contractor agrees to intervene in such lawsuit to protect and assert its claims of privilege against disclosure of such material or waive the same. Contractor further agrees to defend, indemnify and save and hold harmless the City, its officers, agents and employees, from any claim, damages, expense, loss or costs arising out of Contractor's intervention to protect and assert its claim of privilege against disclosure under this Article including but not limited to, prompt reimbursement to the City of all reasonable attorney fees, costs and damages that the City may incur directly or may be ordered to pay by such court.

27. **LEGAL AUTHORITY:** 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 the Agreement. Each person signing and executing the Agreement

on behalf of Contractor represents and warrants that he has been fully authorized by Contractor to execute the Agreement on behalf of Contractor and to validly and legally bind Contractor to all the terms, performances and provisions of the Agreement. The City shall have the right, in its sole discretion, to either temporarily suspend or permanently terminate the Agreement if there is a dispute as to the legal authority of either Contractor or the person signing the Agreement to enter into the Agreement.

28. **NO CONSTRUCTION AGAINST DRAFTING PARTY:** The parties and their respective counsel have had the opportunity to review the Agreement, and the Agreement will not be construed against any party merely because any provisions of the Agreement were prepared by a particular party.

29. **ORDER OF PRECEDENCE:** In the event of any conflicts between the language of the Agreement and the exhibits, the language of the Agreement controls.

30. **SURVIVAL OF CERTAIN PROVISIONS:** The terms of the Agreement and any exhibits and attachments that by reasonable implication contemplate continued performance, rights, or compliance beyond expiration or termination of the Agreement survive the 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.

31. **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.

32. **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.

33. **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 plant, 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 or its officers, directors, employees, agents, vendors or elected officials and/or other substantially similar occurrences beyond the party's reasonable control ("Excusable Delay") herein. In the event of any such Excusable Delay, time for performance shall be extended for a period of time as may be reasonably necessary to compensate for such delay.

34. **PARAGRAPH HEADINGS:** The captions and headings set forth herein are for convenience of reference only, and shall not be construed so as to define or limit the terms and provisions hereof.

35. **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.

36. **COUNTERPARTS OF THIS AGREEMENT:** This Agreement may be executed in counterparts, each of which shall be deemed to be an original of this Agreement.

37. **ELECTRONIC SIGNATURES AND ELECTRONIC RECORDS:** Contractor consents to the use of electronic signatures by the City. The 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 the 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 the 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.

38. **ADVERTISING AND PUBLIC DISCLOSURE:** The Contractor shall not include any reference to the Agreement or to services performed pursuant to the Agreement in any of the Contractor's advertising or public relations materials without first obtaining the written approval of the Manager. Any oral presentation or written materials related to services performed under the Agreement will be limited to services that have been accepted by the City. The Contractor shall notify the Manager in advance of the date and time of any presentation. Nothing in this provision precludes the transmittal of any information to City officials.

39. **PREVAILING WAGES:**

A. Contractor shall comply with, and agrees to be bound by, all requirements, conditions and City determinations regarding the Payment of Prevailing Wages Ordinance, Sections 20-76 through 20-79, D.R.M.C. including, but not limited to, the requirement that every covered worker working on a City owned or leased building or on City-owned land shall be paid no less than the prevailing wages and fringe benefits in effect on the date the bid or request for proposal was advertised. In the event a request for bids, or a request for proposal, was not advertised, Contractor shall pay every covered worker no less than the prevailing wages and fringe benefits in effect on the date funds for the contract were encumbered. Current prevailing wages are attached as Exhibit C.

B. Date bid or request for qualifications/proposals was advertised April 7, 2016.

C. Prevailing wage and fringe rates will adjust on, and only on, the anniversary of the date the Contract was fully executed. Unless expressly provided for in this Agreement, Contractor will receive no additional compensation for increases in prevailing wages or fringe benefits. Contractor shall provide the Auditor with a list of all subcontractors providing any services under the contract. Contractor shall provide the Auditor with electronically-certified payroll records for all covered workers employed under the contract.

D. Contractor shall prominently post at the work site the current prevailing wage and fringe benefit rates. The posting must inform workers that any complaints regarding the payment of prevailing wages or fringe benefits may be submitted to the Denver Auditor by calling 720-913-5000 or emailing [auditor@denvergov.org](mailto:auditor@denvergov.org).

E. If Contractor fails to pay workers as required by the Prevailing Wage Ordinance, Contractor will not be paid until documentation of payment satisfactory to the Auditor has been provided. The City may, by written notice, suspend or terminate work if Contractor fails to pay required wages and fringe benefits.

**EXHIBITS**

**EXHIBIT A-SCOPE OF WORK**

**EXHIBIT B-CERTIFICATE OF INSURANCE**

**EXHIBIT C-PREVAILING WAGES**

**EXHIBIT D-VIDEO VISITATION SCHEDULE**

**ATTACHMENT 1-ENTERPRISE ARCHITECTURE TECHNOLOGY STANDARDS**

**ATTACHMENT 2-SYSTEM REQUIREMENTS**

**ATTACHMENT 3-CCD VIDEO VISITATION RFP BACKGROUND AND OBJECTIVES**

**REMAINDER OF PAGE INTENTIONALLY BLANK**

**Contract Control Number:** SHERF-201734866-00

**Contractor Name:** SECURUS TECHNOLOGIES INC

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:

REGISTERED AND COUNTERSIGNED:

Attorney for the City and County of  
Denver

By \_\_\_\_\_

By \_\_\_\_\_

By \_\_\_\_\_



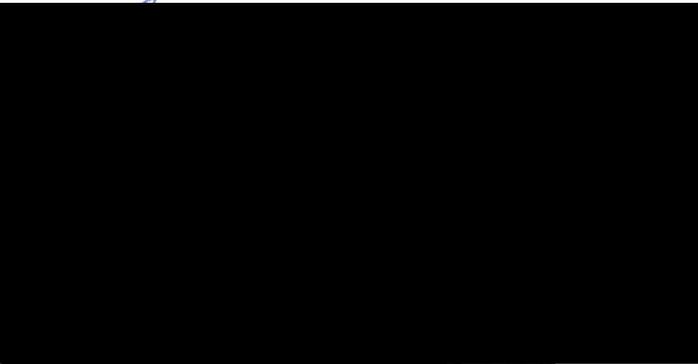
**Contract Control Number:** SHERF-201734866-00

**Contractor Name:** SECURUS TECHNOLOGIES INC

By:

Name:

Title:



(please print)



**ATTEST: [if required]**

By: \_\_\_\_\_

Name: \_\_\_\_\_  
(please print)

Title: \_\_\_\_\_  
(please print)





# Technology Services Program Management Office

Scope of Work

Video Visitation

Technology Services / Denver Sheriff's  
Department

Version: 1.0

Published:

[Publish Date]



# Program Management Office Scope of Work

- Contents
- Document Revision History ..... 1
- Introduction ..... 2
  - Project overview ..... 2
  - Timeline ..... **Error! Bookmark not defined.**
- Objective ..... **Error! Bookmark not defined.**
- Project Management ..... 5
  - Vendor Project Management Responsibilities ..... 5
  - City Project Management Responsibilities ..... 6
  - City Resources ..... 6
- Schedule ..... 6
  - Project Phasing Approach ..... 6
  - M.0: Phase 0 – Project Startup & Baseline Configuration ..... 9
    - M.0.00: Project Startup / Implementation Kick-Off ..... 10
      - Develop Context Diagram ..... 10
      - Create Process Inventory ..... 11
      - Identify & Review Current Systems ..... 11
      - Outline Project Critical Success Factors ..... 11
      - Outline Project Charter ..... 12
    - M.0.01: Pre-Implementation Tasks & Baseline Configuration ..... **Error! Bookmark not defined.**
      - Pre-Implementation Tasks ..... 12
      - Baseline Configuration ..... 12
  - Phase 1 – SECURUS/Video Visitation System Deployment ..... 12
  - M.1.00: Planning and Project Management Deliverables ..... 13
    - Project Charter ..... 13
    - Project Plan ..... 14
    - Risk Register ..... 15
    - Quality Management Plan ..... 15
    - Project Directory ..... 15
    - Change Management Plan ..... 15
    - Communication Plan ..... 16
    - Project Team ..... 16
  - M.1.01: Planning & Design ..... 16
    - Requirements ..... 17
    - Gap Analysis – “Fit Gap” ..... 17
    - Detailed Configuration Requirements ..... 18



## Program Management Office Scope of Work

Determine System Enhancements.....	19
Design Deliverables .....	19
M.1.02: Final Implementation Plan Review & Sign-off.....	<b>Error! Bookmark not defined.</b>
M.1.03: Configuration .....	<b>Error! Bookmark not defined.</b>
Configure System .....	19
Identify New Reports.....	21
Unit Testing.....	23
Create Implementation Plan.....	20
Securus Key Milestone Configuration Activities .....	20
M.1.04: Testing.....	21
Testing Review and documentation .....	22
User Acceptance Testing .....	23
M.1.05: S-Gate User Interface Training / Onsite User Training for City.....	<b>Error! Bookmark not defined.</b>
Outline Training Curriculum .....	25
Development Training Materials .....	26
Develop Quick Guides .....	26
Conduct Training.....	26
M.1.06: Implementation of Services .....	27
Deployment Deliverables .....	27
M.1.07: Final Acceptance .....	28
Documentation.....	28
M.1.08: Post Implementation.....	29
Payment Terms .....	29
Payment and Process.....	29
Pricing .....	29
Contract Sum .....	30
Service Levels .....	30
Service and Support .....	31
Jail Working Conditions .....	33
Appendix C: Follow Up from RFP .....	<b>Error! Bookmark not defined.</b>
Appendix D: Preliminary Implementation Plan.....	48
Acceptance .....	60



Document Revision History

Version	Editor	Date	Summary
1.0	[REDACTED]	3/22/17	Initial Creation and Submission
1.1	[REDACTED]	5/7/2017	Revision

## Introduction

### Project overview

The objective of this project is to replace the Denver Sheriff Department's ("DSD") current video visitation system in two of its detention facilities: Denver County Jail ("COJL") and the Van Cise-Simonet Detention Center -Denver Detention Center ("DDC").

There are currently two different visitation systems in these facilities, both of which are outdated, unreliable, and functionally limited. This scope of work will replace both systems with a single, open-architecture visitation solution. This solution will be implemented in a phased approach. Installation will begin at the DDC and then the COJL. Future phases, as determined by DSD and the City, will include additional functionality and/or integrations.

This Scope will include:

#### PHASE 1- Initial Visitation Function

- Replacement of all existing multi-use kiosks in the DDC
- Installation of new multi-use kiosks in the COJL
- Software that will manage visitation process at DSD
- Several portable visitation stations
- Data transfer from current for inmate location

#### PHASE 2- Expanded Kiosk Functionality

- Phone Call Application
- Inmate Grievance Forms Application
- Inmate Handbook Application
- Third Party Vendor Commissary Application
- Website Education Application
- Inmate Videos Application
- Commissary Ordering Application
- Emergency Visitation Application
- Inmate Sick Form- Medical Kites

Integrations:

- Jail Management System
- Commissary System
- Grievance System
- Inmate Services

- Courts

With a yearly additional application charge

- Job Search Application
- Law Library Application

## 1 Visit Kiosks

### 1.1 Equipment

- a. COJL (Denver County Jail)- DSD plans to replace all the video kiosks in COJL. The vendor shall furnish and install all components of the kiosks including the station itself (seating/desk/partitions), handsets, video cameras, monitors and power sources.
- b. DDC (Downtown Detention Center)- DSD plans to utilize the existing visit stations (seating/desk/partitions) with the new solution. The vendor shall provide and install new video monitors, cameras, handsets and power sources, as needed, into the existing stations

### 1.2 Privacy

Each visit station in the facility lobbies and inmate housing areas shall be configured to provide privacy of the user by preventing eavesdropping and screen viewing by passersby. Measurements of the privacy partitions on each visit station shall, at a minimum, be equal to the measurement of the partitions in the existing DDC visit stations.

### 1.3 Non-Proprietary Components

Visit kiosks shall be assembled from new, non-proprietary electronic components.

### 1.4 Detention Grade Equipment

- a. All components of the visit kiosks (in both inmate housing and lobby areas and portable units) including seating, privacy partitions, handsets, shall be detention grade and intended for use in a maximum-security detention environment, whereby they are abuse resistant, tamper proof, vandal proof, and have a graffiti-resistant finish.

- b. All visit stations in the inmate housing areas shall include a seating component (excluding ADA kiosks) for use by the visit participant that is stationary and permanently affixed in place at the visit station.
- c. The video monitor and camera for each visit kiosk shall be encased in abuse-resistant enclosures made of detention grade, scratch resistant metal and shatterproof, scratch-resistant monitor and camera screens, all made of detention grade materials and mounted into the kiosk.
- d. Visit handsets used by visit participants shall include a cord that meets detention-grade standards (in length and materials).

#### 1.5 Portable Stations

The vendor shall provide portable visit stations (2 per facility) for each facility for use in the medical and special management units where inmates may be confined to a bed or a cell.

### 2 Kiosk ADA Compliance

#### 2.1 The solution shall support compliance with applicable ADA requirements by:

- a. Providing inmates and visitors who have disabilities physical access to, and the ability to operate, visitation equipment.
- b. Providing user functionality, video and audio that support the ability for visit participants with disabilities to communicate clearly with each other.

#### 2.2 Portable Visit Stations

The solution shall provide portable visit stations that are also ADA compliant.

### 3 Kiosk Construction and Installation

- 3.1 The vendor shall furnish, install, and maintain all video visitation equipment including hardware, software, and network components.
- 3.2 The vendor shall furnish all necessary labor, tools, equipment, and supplies related to completing the installation of the solution.

- 3.3 The vendor shall be responsible for obtaining all permits and inspections (including the cost thereof) that are required by government authorities to complete installation of the solution.
- 3.4 The vendor shall clearly, logically and permanently mark all components of the system so that they can be easily identified by the City. Components may include, but are not limited to, switches, connectors, jacks, receptacles, outlets, cables, and cable terminations.
- 3.5 The installation shall follow the City of Denver Building and Fire Codes.
- 3.6 The vendor shall be responsible for performing all equipment and system testing, adjustments as necessary to ensure system functionality.

#### **4 Project Management**

##### **4.1 Vendor Project Management Responsibilities**

- a) Coordinating the development of the project plan in consultation with the CCD project manager and team members.
- b) Managing, in conjunction with CCD PM where applicable, escalations where needed.
- c) Management of Securus will partner with all project resources and teams to ensure the timely delivery of items identified as "In scope" within this SOW.
- d) Ensuring that members of the City staff are sufficiently educated in the Securus applications to understand the implications of initial design decisions.
- e) Providing the City with timely and detailed descriptions of the items identified as "City task" within this SOW.
- f) Advising the City of expected completion dates for items identified as "City task" within this SOW.
- g) Advising the City of the impact on the expected delivery dates of "City task" items when prerequisite City tasks, such as the completion of data import templates or approval of report specifications, are advanced or delayed.

- h) Monitoring the progress of the project and advising the City of risks to its on-time completion.
- i) Coordinating the completion and approval of change orders.

#### 4.2 City Project Management Responsibilities

- a) The timely delivery of items identified as “City task” within this SOW.
- b) Advising Securus of expected delivery dates for items identified as “City task” within this SOW.
- c) Ensuring that change orders contain a full specification of the changes required.
- d) Ensuring that customizations are fully specified and documented.
- e) Ensuring that all City team members have a clear understanding of their responsibilities to the project.

#### 4.3 City Resources

The requirement for City resources is variable with:

- The duration of the project.
- The degree of internal City consultation.
- The level of internal City agreement.
- The number of customizations.

### **5 Schedule**

#### 5.1 Project Phasing Approach

Securus (also known as “the vendor”) will utilize the following phased transition plan with the intent of being ready to implement Video Visitation for the Denver Sheriff Department in accordance with mutually agreed timeframe, from Contract execution. The proposed phases are described below.



## Program Management Office Scope of Work

The City and County of Denver (CCD or the City) is implementing a new video visitation solution with the vendor that can meet all the requirements outlined below in the "Agreed Requirements" section. Additionally, any future configurations and reporting requests may be requested.

The following sections outline the detailed plans for the phases of our overall implementation plan:

Phase 0: Project Startup & Baseline Configuration

Phase 1: Securus Video Visitation System Deployment

- Securus Video Visitation Application
- Securus Video Visitation System Deployment
- Phone Call Application
- Basic Integration with JMS for inmate movements

Future Phases as determined by the City to implement:

- Inmate Forms Application (Grievance)
- Inmate Handbook Application (.PDF)
- Third Party Vendor Commissary Application
- Website Education Application (URL)
- Inmate Videos Application (.MP4)
- Self-Op Commissary Ordering Application
- Emergency Visitation Application
- Inmate Sick Form
- Job Search Application (annual per App charge)
- Law Library Application (annual per App charge)

Integrations:

- Jail Management System
- Commissary System
- Grievance System
- Inmate Services
- Law Library
- Courts

### Milestone Timeline

	Milestones	Scheduled Completion
<b>Milestone 0</b>	Project Startup & Baseline Configuration	7 days from contract execution
	Project Startup / Implementation Kick-Off	1 days from Project Kick off

	Pre-Implementation Tasks & Baseline Configuration	7 days from Project Kick off
<b>Milestone 1</b>	<b>SECURUS/Video visitation System Deployment</b>	<b>74 days from Project Kick off</b>
1.0	Planning & Project Management Deliverables	Continuous throughout Phase 1
1.1	Planning & Design	32 days from Project Kick off
1.2	Final Implementation Plan Review & Sign-off	39 days from Project Kick off
1.3	Configuration	52 days from Project Kick off
	Configuration - Pre-Installation Preparation / Customer provisioning completed	30 days from Project Kick off
	Configuration - LEC MPLS T1 Installations / LEC Delivery. Turn-up Prep	48 days from Project Kick off
	Configuration - Pre-Transition Installation Activities / Onsite wiring, equipment installation, terminal replacements	52 days from Project Kick off
1.4	Testing	59 days from Project Kick off
1.5	S-Gate User Interface Training / Onsite user training for City	62 days from Project Kick off
1.6	Implementation of Services	67 days from Project Kick off
1.7	Final Acceptance	74 days from Project Kick off
1.8	Post Implementation	30 days from Project Implementation

The above indicated timelines are adjustable per need; with communication and agreement from the City and County of Denver and Securus. The City and County of Denver reserves the right to not proceed on future phases for any reason. There shall be no financial obligation for CCD with regards to deciding not to proceed with future phases as outlined above in the project phases. Similarly, all future phases, as outlined, are included in the current cost structure as outlined in the “Financial Breakdown” section within this document.

Should the City and County of Denver decide to continue with future phases (Other Securus Modules) the vendor shall be ultimately responsible for providing access and resources for enabling, configuring, training, and supporting new modules within the Securus Video Visitation system.

The implementation of each Securus phase will involve the following:

- a) An overview of, and training in, the functionality and the ways in which the functionality can be extended by configuration and customizations – and onsite training in how to do so.

- b) A determination of how best to configure and, if necessary, customize to meet the objectives of the City.
- c) An overview of the advantages and, if present, disadvantages of the proposed configuration and customizations, along with recommendations and assistance in developing or changing business processes if necessary.
- d) Documentation of the agreed configuration and customizations.
- e) Determination of custom reporting requirements that cannot be met by the standard reports – and assistance in building those falling into agreed deliverables / requirements, or change orders for all others.
- f) The preparation of change orders including the specifications for any required custom reports.
- g) The development by Securus of any required custom reports.
- h) The testing and acceptance by the City of custom reports and ad hoc models.
- i) The deployment of custom reports and ad hoc models.
- j) The development of an integration strategy for any integrations with Securus,
- k) The development by the City of the integration components that are required.
- l) The development by Securus of all integrations, configuration or customization.
- m) The deployment of all integrations, configuration, or customization.
- n) The testing and acceptance by the City of the integrations, configuration or customization

#### Phase 0 – Project Startup & Baseline Configuration

Securus will commit the required resources to begin project startup and initial requirements gathering activities during full lifecycle of project implementation. Securus will work with the City to establish the project infrastructure, gather

business/functional and technical requirements, setup a baseline configuration and analyze any source system data.

#### Project Startup / Implementation Kick-Off

The Securus project team, led by the Contractor Project Manager (CPM) will be responsible for initial setup and ongoing coordination of the following items and activities in support of the project:

- Coordinate and manage the activities of Contractor's project personnel
- Maintain Contract communications through CCD's Project Manager, including a communication plan that will define the steps, processes and tools utilized to communicate project information to CCD employees and senior management
- Collaborate and develop a project work breakdown structure and schedule
- Develop a project charter (e.g., business objectives, project scope, program solutions, governance and project structure, success factors, milestones and risk management plan)
- Create and communicate a project directory (resources and contact information associated with the project)
- Develop a risk register to provide a format for recording project risks that can be discussed during weekly quality review meetings as well as a monthly risk assessment meeting
- Frame a structure to discuss change management to define how modifications to the statement of work and agreed upon requirements will be evaluated, changed and coordinated
- Define the steps and processes to be utilized to ensure a sufficient level of quality is maintained throughout the life of the project within a quality management plan
- Securus Kick-off Transition Plan Meeting

During the project startup phase, the structure will be put in place to support all the above activities through the remaining phases of the project.

The project startup phase will be largely focused on reviewing the entire scope of the multi-phase project to drive the planning and scheduling of the remaining project phases. Securus will work through the City and County of Denver Project Manager to conduct a range of meetings with all the key stakeholders (as defined by the CCD Project Manager) and focus on the below activities (among others per City need as it arises) during the project startup.

#### Develop Context Diagram

The purpose of the context diagram is to provide a graphical, high-level overview of all the key stakeholders, the core processes/functions, and the interactions

between the stakeholders and the core processes/functions. The purpose of the context diagram is to provide an easy to understand, visual depiction of the entire scope of the project. The context diagram is used throughout the project during allow project participants to maintain a solid understanding of how each detailed activity completed with the project fits into the broader scope of the project.

### Create Process Inventory

The City and County of Denver Business Analyst and Project Manager will work with Securus and Denver Sheriff Department (DSD) to identify and itemize all the specific processes that will need to be supported. The details of each process will be captured as input for the later phases of the project. The City and County of Denver assigned Business Analyst will provide all captured process documentation and will engage in and coordinate the gathering of any additional process information. The information utilized in the vendor process inventory will ultimately be produced by and/or provided to the City and County of Denver Business Analyst. The City and County of Denver Project Manager and Business Analyst will lead this effort, working with Denver Sheriff Department and Securus to capture this information.

### Identify & Review Current Systems

The City and County of Denver Project Manager and Business Analyst will work with Securus and DSD to identify and itemize all the current systems that support the various processes identified in the process inventory. Securus is responsible for details on the system that will be captured, provided to and approved by the City and County of Denver assigned Business Analyst and utilized as input for the later phases of the project. The vendor shall work on this effort, in coordination with the City Project Manager, through the City and County of Denver assigned Business Analyst (who will engage in and coordinate all information gathering / documentation related to the project). The City and County of Denver Project Manager and Business Analyst shall facilitate these sessions with the vendor documenting all information. The vendor shall adhere to the requirements standards (with regards to format and content) as defined by the City later. The vendor shall obtain approval from the City Project Manager before a deliverable is complete. The City and County of Denver is the owner of all documentation produced (be it by a City resource or a vendor resource) with regards to requirements that touch City processes. All original documentation shall be kept by the City and County of Denver. All updates required for the documentation in the future shall be updated in the original source that is owned by the City.

### Outline Project Critical Success Factors

The City and County of Denver Project Manager and Business Analyst will work with DSD and Securus to identify and itemize the project's critical success factors

(CSFs). The details of each CSF will be captured as input for the later phases of the project.

### Outline Project Charter

Securus will work with the City and County of Denver Project Manager to create the project charter that will include the following:

- Business objectives
- Scope overview
- Integrated business solution
- Integrated governance and project structure
- Project critical success factors
- Milestones
- Risk management plan

### Pre-Implementation Tasks

Securus will complete the following tasks

- Site Inspections
- Initial Telecom & Equipment Orders

### Baseline Configuration

Many of the requirements for Phase 1 will be supported using baseline features of Securus that can be enabled through relatively simple configuration activities. The purpose of the baseline configuration activity is to identify and document the configuration required to support many of the project requirements with "out-of-the-box" functionality. The baseline configuration will be completed and utilized as the starting point for the more detailed requirements gathering, configuration management, and customizations required for the later phases of the project.

### **Phase 1 – Kiosk Replacement/ Installation and Securus Video Visitation System Deployment**

Phase 1 will be focused on implementing Securus' SECURUS/Video Visitation module at the Denver Sheriff's Departments (DSD) COJL (County Jail) and DDC (Denver Detention Center) At the completion of this phase, City and County of Denver employees and Inmates will be fully trained to utilize Securus Video Visitation for the Core Processes required for Video Visitation functions. This phase of time is estimated at approximately 90 days from contract award.

The City shall have the right to request new resources from Securus should the City deem they are not a good fit for the project, with the changes in resources being as immediate as possible.

The vendor is expected to provide a project team that is responsive to CCD contact, is on time to status meetings (and attentive / engaged), meets commitments, and communicates effectively.

During each phase of the project, the vendor project manager, in coordination with the CCD Project Manager, shall utilize and continually maintain the project management components that were initially set up during the project initiation.

All future phases will follow Initiation, Planning, Execution, Monitor and Control, and closing as well as the same deliverables as described within the Scope of Work.

#### Planning and Project Management Deliverables

During each phase of the project, the vendor project manager, in coordination with the CCD Project Manager, shall utilize and continually maintain the project management components that were initially set up during the project initiation.

#### Project Charter

The project charter will guide the project as each phase unfolds and any new information that affects the project charter shall be used to refine the project charter as necessary during each project phase. Securus, in coordination with the City Project Manager, shall assist in creating the initial Project Plan as needed to satisfy the City's documentation, reporting and oversight requirements. The items that follow are subsections within the Project Charter template:

- a) Business Objectives – Shall list the high-level project objectives for this scheduling project.
- b) Scope Overview – Shall list the high-level goals for this scheduling project.
- c) Integrated Business Solution – Shall detail how the high-level goals will be integrated to ensure a well-designed foundation for People Soft and other potential enterprise applications.

- d) Integrated Governance and Project Structure – Shall detail the key resources, roles and responsibilities sufficient to support project completion.
- e) Project Critical Success Factors – Shall list the key project factors that should be observed to deliver the project on time and within budget.
- f) Integrated Milestones – Shall list the high-level tasks necessary to fulfill the contractual obligations of this project.
- g) Risk Management Plan - Shall document and communicate known risks and evaluate potential risks in all phases of the Contract. The plan shall include mitigation strategies and establish the framework for identifying, managing and controlling risks. It shall also reflect how Securus defines risk, impact and probability.

## Project Plan

Securus shall create in consultation with the CCD Project Manager a high-level project plan during the project initiation. Integrated Project Plan (Work Breakdown Structure): Securus shall provide details on work that will be completed in each Contract phase, the amount of time expected to complete each task, and the staff or resources assigned to complete each task during the planning phase. At a minimum, this plan shall include an estimated but complete resource loaded schedule, including any constraints or assumptions. Securus shall employ professional project management software such as Microsoft Project. The Project Plan shall be used to guide the work for each phase. At the beginning of each phase the specific details for each phase will be revisited and shall be expanded upon to provide greater details for the project activities for each phase.

As part of the project plan, go live will be tentatively stated. Due to the complexity of the project and the various phases it entails, the go live date will be flexible as agreed upon by the vendor and the City and County of Denver.

Delivery dates for project deliverables shall be negotiable and agreed upon by the vendor and the City and County of Denver. Early in the requirements development for the deliverable an estimated delivery date range shall be provided by the vendor. Once requirements are completed, a commitment date shall be provided by the vendor to CCD. The vendor shall deliver within a +/- 15% window of the commitment date.

## Risk Register

Securus shall provide the format for recording project risks. The project risk register will be created by Securus and maintained jointly with CCD PM. The risk register shall be utilized to manage known risks as each phase unfolds and any new information that affects the project risk register will be used to refine the risk register as necessary during each project phase. Risks will be discussed during weekly project meetings (including CCD PM, CCD BA, DSD, and Securus).

## Quality Management Plan

The quality management plan shall define the steps / processes to be used to ensure a sufficient level of quality is maintained throughout the life of the project. This shall drive the quality assurance for the project as each phase unfolds and any new information that affects the quality management plan shall be utilized to refine the plan as necessary during each project phase.

## Project Directory

Securus and City shall list the resources and their contact information associated with the project. The project directory shall be created by the City and County of Denver Project Manager and will be used throughout all phases of the project and updated as necessary when there are changes to the project team. The vendor shall inform the CCD Project Manager of all changes that occur on the vendor project team so that this information can be accurately reflected within the project directory.

## Change Management Plan

Securus shall help the City develop an appropriate change management strategy that at a minimum will:

- a) Identify and fully articulate the organizational changes that the initiative will bring;
- b) Develop specific transition and communication strategies for the various stakeholder groups;
- c) Develop strategies for mitigating and managing major barriers for implementation;
- d) Define how changes to the SOW and agreed requirements are to be evaluated, changed, and coordinated within the contract,
- e) Work with City counterpart(s) and communication support staff.

- f) Ensure all solutions, updates and changes are tested in a TEST environment and have a rollback plan agreed upon by CCD.

Any new information that affects the change management plan will be used to refine the plan as necessary during each project phase. The change management plan shall be maintained by the CCD Project Manager in conjunction with input from the vendor's project manager and agreement from the vendor.

### Communication Plan

Securus shall assist in defining the steps / processes / tools available to communicate project information to City Project manager and key stakeholders. Communication to City employees is the sole responsibility of the City. The communication plan will be utilized to manage communications throughout the project. Any new information that affects the communication management plan will be used to refine the plan as necessary during each project phase. The communication plan shall be maintained by the CCD Project Manager in conjunction with input from the vendor project manager.

### Project Team

The City and County of Denver reserves the right to dismiss a vendor project team member if they no longer meet the expectations of the City as defined by this statement of work.

The vendor is expected to provide a project team that is responsive to CCD contact, is on time to status meetings (and attentive / engaged), meets commitments, and communicates effectively. Resources allocated to the project shall be knowledgeable of the product, our business processes (as defined and provided in the "Agreed Requirements" section of this document) and shall be fully capable of performing their duties as assigned. Should a resource not can fulfill their responsibilities the City reserves the right to remove a team member (for any reasonable reason) from the project. If a vendor team member is removed the vendor shall provide a more capable resource and assign them to the project in the same capacity as the previously removed resource. The new resource shall be provided to the City within 3 business days of the previous resource removal.

### Planning & Design

Securus Video Visitation Project Manager, in coordination with CCD Project Manager will be coordinate the following design activities:

Survey and document the Sheriff's departmental business processes (identifying any gaps in current process documentation), accounting processes, and identify different documents that will need to be created as part of the deliverables. All documents and related information that is identified by the vendor as necessary shall be agreed upon and approved by the City.

The documents (and their related information gathering) shall be facilitated by the CCD Business Analyst, documented by Securus, and provided to the City by the vendor.

The CCD Business Analyst shall work alongside the vendor in the process of gathering this information (though the vendor will be responsible for its creation). The vendor shall provide all documentation to the City in its original form. All changes to the documentation shall be performed within the original City owned documents.

The documentation produced by the vendor shall adhere to the requirements standards (format and content) as defined by the City and County of Denver. The City shall provide the standards information to the vendor once the information gathering commences. This is so that ultimately the process knowledge exists first within City and County of Denver resources, is owned by CCD and is created and maintained in current CCD business process formats for future projects that need to make use of the information.

Familiarize the team(s) with the current database and collaborate/create a data migration plan, including reports and data migration methodologies to define various details of the software implementation

## Requirements

The CCD Business Analyst, in coordination with Securus will document the future business requirements (those identified as additions to the current produced documentation) for each of the supported processes, including specific changes being made that will alter existing processes.

## Gap Analysis – “Fit Gap”

Securus will work with the City to conduct a fit-gap analysis to determine what solution functionality best meets the City's requirements; as specified in the functional and technical requirements documents.

- a) Securus will assist with and be responsible for documenting the final gathering of the business requirements.
- b) Securus will be responsible for creating the final list of functional and technical requirements if applicable.
- c) Securus will be onsite for the duration of requirements gathering.
- d) Any gaps in functionality with the City's requirements shall be communicated to CCD Project Manager. Any gaps shall be mutually agreed upon.

The vendor will perform analysis to define the gaps between the CCD requirements and the standard Securus capabilities. Each identified gap will be identified to be addressed through enhancements to Securus. The vendor shall produce a full fit gap document to the CCD Project Manager. The CCD Project Manager and Project Sponsors will decide whether the identified fit gap items shall be included as scope change

#### Implementation Plan Review & Sign-off

Upon completion of the kick-off meeting, Securus will submit an updated plan to CCD points of contact for review and approval. Immediately upon approval, the plan will be implanted for all approved sites. Securus will follow the procedures as detailed within the document and refined based upon CCD input, to complete an on-time transition of all systems, hiring of all on-site personnel, and training of all system users.

#### Detailed Configuration Requirements

The vendor will document configuration details that will need to be made in Securus to support all the CCD requirements. The configuration requirements shall be provided by the vendor to the CCD Project Manager and CCD Business Analyst. Any changes to schedule and or scope based on the details learned through the production of the configuration requirements shall be understood and agreed upon by the CCD Project Manager, CCD Business Analyst and CCD key stakeholders (as defined by the CCD Project Manager) before the project proceeds.

#### Specifications

Before Securus undertakes any customizations described herein, the City and Securus shall prepare and sign-off on the detailed specifications ("Requirements") for the work to be performed.

## Determine System Enhancements

The vendor will document enhancement details that will need to be made to SECURUS to address each of the gaps identified in the gap analysis (“fit gaps”). The system enhancements shall be provided by the vendor to the CCD Project Manager. Any changes to schedule and or scope based on the details learned through the production of system enhancements document shall be understood and agreed upon by the CCD Project Manager and Project Sponsors.

## Design Deliverables

Securus shall provide City with the following:

- a) Technical architecture design documentation.
- b) Securus shall assist City to review form business rules and policies. Based on that review, Securus shall use this information to form the Software during Configuration.
- c) Data migration design: Work to include analysis of legacy systems to be migrated to the Software.
- d) Reports Review requirement: Securus will verify that the standard reports available from Video Visitation meet reporting requirements. If any requirements are not met, Securus will work with DSD to define specific custom reporting needs at no additional cost following implementation.
- e) Securus will be responsible for creating the configuration guide-detailing how to configure the system when applicable:
  - 1.) Includes architecting workflows;
  - 2.) Includes module configuration per the requirements document; and,
  - 3.) Includes basic onsite training around the same.
- f) Securus will develop mutually agreed upon Service Level Agreement (SLA) and performance metrics
- g) Securus will assist in developing and documenting test plans and scripts for system and user acceptance testing.

## 7 Configure System

Securus shall be responsible for initial software configuration and/or customization based upon the City's agreed requirements in preparation for initial user testing. Securus will apply the documented configuration and/or customization changes to Securus

#### Create Implementation Plan

Securus will work with the City and County of Denver Project Manager and Business Analyst to define the detailed implementation plan. The vendor shall produce and provide this plan to the CCD Project Manager. The deployment plan shall be agreed upon by the vendor and the City prior to implementation

#### Securus Key Milestone Configuration Activities

- Pre-Installation Preparation- Customer provisioning completed
- LEC MPLS T1 Installations- LEC Delivery. Turn-up Prep
- Pre-Transition Installation Activities- Onsite wiring, equipment installation, terminal replacements

Securus shall:

- a) Configure the Software to meet City agreed requirements as determined by the FGR; including the creation and configuration users, groups and roles.
- b) Provide training on and assistance in creating and configuring user and role permissions.
- c) Configure Software with Business Rules and workflows as determined during the Planning and Design phases and by using the FGR.
- d) Create additional reports as needed and identify which fall into agreed deliverables / requirements, or change orders for all others.
- e) Create and configure any DSD specific information as outlined in the requirements and FGR.
- f) Implement integration with IDM (Oracle) to authenticate to Safety domain.
- g) On-the-job onsite training for City personnel for Software configuration.
- h) Preliminary testing of the Software configuration to ensure the Software functions accurately. Securus shall assist the City with the testing of the Software configuration.
- i) Provide a configuration document detailing system interfaces as applicable

- j) Provide (and maintain) three environments (Development, QA, and Production).
- k) Securus will be responsible for any custom development to meet requirements referenced within this SOW. For any custom development, Securus will need to provide technical specifications.
- l) Securus will work with the City to configure the system including:
  - a. Forms for data entry;
  - b. Configure workflows;
  - c. Configure user access/security; noting,
- m) Securus will work with the City to build interface(s) to and from all identified systems. Securus will be responsible for developing the interface(s) in/out of the SECURUS system. The City will be responsible for coordinating with appropriate vendor systems to develop the interfaces in/out of SECURUS.
- n) Securus will work with the City to connect and integrate with the ancillary technical systems (i.e. identity management, etc.) as per technical requirements
- o) Securus will be responsible for initial software configuration based upon the CCD requirements. The configuration activities will include (but not be limited to):
  - Creating and configuring user and role permissions
  - Configuring business rules
  - Creating additional reports as needed
  - Providing on-the-job training for CCD personnel
  - Testing of the software for functionality
  - Assisting CCD with other aspects of software testing
  - Providing a configuration document that details system interfaces

## 8 Report and Reporting

Securus will, in coordination with the City to identify the set of required reports. The vendor shall provide all reports at no cost to the City and County of Denver. The vendor shall also produce all future reports at no cost to the City and County of Denver.

- a. Analytical reports as defined in fit-gap summary;
- b. Documentation on user creation of ad-hoc reports.

## 9 Testing

Securus will be responsible for conducting comprehensive functional testing, including assistance in the development of a test plan that ensures the SECURUS software delivers the expected results that CCD requires, including test script templates; actual service requests; creating financial reports; resolving discrepancies and making configuration changes as needed. Securus and the City will mutually agree on a time frame to resolve discrepancies once reported by the CCD. Securus will provide a resolution for an issue within 5 business days for each reported item. This shall be the applied timeline unless an adjustment to it is communicated and mutually agreed upon by CCD and Securus. The below severity user acceptance testing service level agreements and post implementation support agreements supersede this statement.

The vendor shall develop a test plan that shall be provided to the City and County of Denver and signed off on before any type of implementation / testing begins on the system.

The test plan shall define the definition of done for each product feature and the vendor shall be responsible for meeting all criteria that is established to call a feature fully tested, signed off on, and "done".

The definition of done shall be defined as the following:

- a) Unit tested (and signed off on by to be identified CCD employees)
- b) Integration tested (and signed off on by to be identified CCD employees)
- c) Regression tested (if applicable, and signed off on by to be identified CCD employees)
- d) Solution / system tested (and signed off on by to be identified CCD employees)
- e) User acceptance tested (and signed off on by to be identified CCD employees)

The City and County of Denver reserves the right to request evidence of the above testing types taking place on initial features, future features, configuration items, and during user acceptance testing. The vendor shall fully test to the above identified types whenever work is being done for the City and County of Denver.

#### Testing Review and documentation

Securus will be responsible for development of test script templates for confirming that the configuration changes and enhancements made to SECURUS are working as expected. Securus shall review and modify the initial

Software configuration to address any Fit Gaps and errors identified during all testing phases per the following:

- A) Securus shall review with the City identified Fit Gaps.
- B) Securus shall review with the City, errors and their respective fixes discovered during testing.

### Unit Testing

Securus will be responsible for conducting unit testing for each configuration change and each enhancement made to SECURUS. Unit testing must be successfully completed prior to user acceptance testing and training.

### User Acceptance Testing

Securus will be responsible for the unit testing and reviewing all functionality with the City prior to User Acceptance Testing (UAT). Securus will work with the City and County of Denver Project Manager to define the acceptance testing requirements, scripts, and acceptance criteria. Securus shall participate in resolution of items identified in unit/system and user acceptance testing. Any discrepancies not in alignment with the original requirements will need a mutually agreed upon resolution. Securus may be required to provide documentation.

### Bugs and System Flaws

Bugs shall be classified into three severity categories (each with an associated SLA)

Severity 1 – stoppage of additional testing (within a unit OR the system)  
Bugs classified as severity 1 shall be the first focus of the vendor in terms of resolving. Severity 1 bugs shall be resolved within 24 hours.

Severity 2 – impacting additional testing but a work around exists  
Bugs classified as severity 2 shall be secondary focus of the vendor in terms of resolving. Severity 2 bugs shall be resolved within 72 hours.

Severity 3 – not impacting additional testing but must be resolved and tested before launch  
Bugs classified as severity 3 shall be third focus of the vendor in terms of resolving. Severity 3 bugs shall be resolved within 5 business days.

Severity 4 – not impacting additional testing, and system may (if CCD agrees) be allowed to launch with the bug in place  
Furthest down with regards to vendor focus. These should be considered only if there are no severity 1, 2 or 3 bugs still open.

Securus shall be accountable to the above service level agreements associated to each severity level. Adjustments to the service level agreements shall be granted on a one-off basis and shall be communicated and mutually agreed upon by the vendor and City and County of Denver. The city reserves the right to accept or reject service level agreement adjustment requests for any reason.

The City and County of Denver reserves the right to classify a bug into one of the above categories as we see fit. There shall be no adjustments to bug severity by the vendor without first consulting the identified CCD Project Manager.

CCD shall test and sign off on bugs as they are resolved. Bugs shall not be closed out as resolved until the sign off from CCD is obtained.

CCD shall not be restricted to testing only per script guidance. All bugs identified by CCD shall be resolved in accordance with the SLA.

Usability flaws found by CCD that are deemed change requests (or small enhancements / change of behavior) by CCD shall be classified as bugs.

Performance related flaws (that are identified as caused by the vendor) shall also be classified as bugs. The City and County of Denver reserves the right to determine what constitutes a performance bug.

As part of acceptance testing CCD will also be testing in a security capacity. All security concerns / flaws shall be classified as bugs. Security bugs could fall into any application layer.

Traditional application bugs (where the application does not perform as designed OR would be expected by a reasonable person to perform) shall be classified as bugs. The City and County of Denver reserves the right to determine what reasonably expected design / functionality of an application is.

The City and County of Denver reserves the right to determine which (if any) bugs are acceptable to launch the application with. As a general guideline, there shall be no severity 1, 2, or 3 bugs remaining when launching the application officially for production use. The City reserves the right to adjust this policy as it sees fit.

The vendor shall put forth their best effort to meet the above defined SLA's per severity level. All exceptions to the above SLA's shall be communicated to the City and County of Denver Project Manager. The vendor shall provide just cause for the exception request and shall provide the timeline for the extension request (i.e. when they will deliver the resolution for the bug). The City and County of Denver shall consider each exception request and reserves the right to approve or reject such requests after reasonable consideration.

## 10 Training

Securus commits to design and conduct training for CCD to familiarize all relevant job functions with the SECURUS software. Securus shall provide on-site training. The training shall be designed and conducted to provide familiarization in all aspects of the Software by job function. The City will utilize train-the-trainer approach for end-user training. Training will be scheduled through agreement between Securus and the City.

- a) All training shall be conducted against a DSD-specific non-production database
  1. Training to be provided against a final state non-production environment that is stable and UAT complete.
  2. There shall be no outstanding bugs / enhancements in open status prior to conducting training. This is to avoid training a user on an incomplete system that will be changing soon post training (thus requiring a training refresher).
- b) The training approach shall be flexible enough to allow the City to adjust the participants and curriculum to achieve the greatest benefit for the training.
- c) Securus shall submit to the CCD Project Manager for approval a class outline and training manual, along with time estimate to complete the sessions.

A qualified technical expert shall conduct all training. The instructor(s) shall have a thorough mastery of the specific subject matter involved and shall can impart information to others in easily understood terms and with DSD-specific scenarios.

### Outline Training Curriculum

Securus will develop training class outlines and training manuals, along with time estimates to complete the sessions. The online training developed by the vendor shall cover 100% of the functional units within the impound system (and any customized components added based on CCD need). The vendor shall also complete a series of online training courses for Video Visitation and all modules/components.

The online training developed by the vendor shall cover 100% of the functional units within the dispatch system (and any customized components added based on CCD need).

The online training shall be web based and in a video format that guides the user through each piece of the system (showing screens and use case steps through each of the system components).

### Development Training Materials

Securus will develop user manuals for use by CCD with specific training modules based on the SECURUS software functionality, including one (1) hard copy of each training manual and one (1) electronic copy of each training manual in Microsoft Word format. The CCD may create as many copies of the training manuals as needed for its internal use. The electronic version of the training manual shall be accessible from within the associated software component.

### Develop Quick Guides

Securus will create quick reference guides (no more than a total of two (2) pages in length), including graphics for all relevant job functions. These quick reference guides shall be provided to CCD in electronic format and shall be accessible from within the associated software component.

### Conduct Training

Securus will conduct live and interactive training sessions for CCD identified staff that will cover the essential concepts and standard navigation of the SECURUS software, as well as end-to-end business processes including, but not limited to, creating a service request, entering information in a service request, assigning service requests, cashiering, and report generation. Securus agrees to provide class room training on-site at CCD specified locations, including various locations within a ten (10) mile radius of Denver. Securus agrees that the training approach shall be flexible to allow CCD to adjust the participants and curriculum.

The vendor will provide training in the following forms:

- Train the trainer
- Train the user

The vendor shall provide refresher training in one or both above forms as needed by the City and County of Denver (not to exceed one on site visit per 6 months).

Onsite training provided by the vendor shall last three full working days and shall provide the attendees with no less than 1 trainer per 8 trainees. The trainees shall have the option to request additional time spent on system units that are less understood by them. The third day of training shall focus primarily on the lesser understood system units that needed additional coverage.

All training materials utilized during the onsite training shall be provided to all trainees within 48 hours of training completion.

Training shall be provided separately for administrative functions and the CCD identified trainees for those functions.

Training shall be provided by vendor appointed trainees. These trainees must have mastery level knowledge of the system and each of the functional units within the system. The City and County of Denver reserves the right to request a new trainer if the provided trainer is not meeting trainee needs. The vendor will supply a new trainer and reschedule training within 48 hours of such a request for replacement. The vendor will be responsible for all costs involved in the replacement of a trainer.

### Implementation of Services

As noted above, Securus will work with CCD Project Manager and Business Analyst to define the detailed implementation plan. Securus shall address and fully test all City agreed requirements as documented, including Fit Gap report, prior to Software deployment. A Deployment Plan will be developed during the Configuration deliverable. This plan, once approved by the City and following successful testing, will result in the software being deployed in the production environment and the plan will detail the order of the divisions and/or facilities that will be deployed.

Successful testing shall be defined as no bugs remaining in the severity 1, or 2 classifications as defined above in the "Acceptance testing" section. CCD may agree to sign off on testing with severity 3 or 4 bugs in place. CCD reserves the right to escalate the severity level of a bug or determine which bugs will be permitted to remain in place for implementation and which will not.

## 11 Deployment Deliverables

- a) Securus shall make best efforts to fix all errors (classification of severity 3 or higher) within five (5) business days after City reports the error.
- b) Securus shall provide architecture diagram, deployment document, and software configuration documentation around key and global settings specific to the City's configuration.
- c) Participate in a go/no go decision with identified stakeholders from the City.
- d) Implement cutover plan to deliver a configured Video Visitation Systems for the Denver Sheriff Department.

- e) Onsite support for 30 business days after production deployment.  
Scheduling to be determined by City (based on Securus availability).

## 12 Final Acceptance

The final Acceptance will be based on successful implementation of the system in the agreed environments and upon successful User Acceptance Testing of the system and its interfaces. Successful testing entails that the system performs as per the agreed requirements, including FGR.

### Documentation

Before the project can be considered closed (beyond the above-mentioned acceptance testing criteria) the following shall be delivered to the City and County of Denver by the vendor:

- Technical administration
- Software configuration
- Interface(s)
- Technical architecture diagram(s)
- Database setup and maintenance
- Data model
- Application administration guide
- End-user day-to-day operation
- Job function quick reference guides
- Finalized and signed off on business process / business requirements documentation

### Close-Out Process

- Close out invoicing;
- Finalize and deliver remaining documentation, recorded trainings, etc.;
- Work with City to conduct Lessons Learned;
- Complete transition to Support and Maintenance and communicate support plan.

Final Acceptance Certificate shall be assigned by the Project Sponsor(s).

### 13 Post Implementation

#### Payment Terms

Payment terms for the Video Visitation implementation are as follows:

- DSD to pay \$420,000 30-days after implementation
- Remaining balance of \$992,000 paid out equally and annually over the final 4-years of the agreement

#### Payment and Process

CCD and Vendor agree to the following fees, collection process and disbursement.

Facility	Total Cost
COJL	895,467
DDC	516,533
<b>Total 5 Year Commitment</b>	<b>1,412,000.00</b>

Year			Payment
<b>1 (30 Days after Implementation)</b>	2018		\$420,000.00
<b>Balance</b>			\$992,000.00
Year			Payment
2	2018	Due 365 days from Year 1 payment	\$248,000.00
3	2019	Due 365 days from Year 2 payment	\$248,000.00
4	2020	Due 365 days from Year 3 payment	\$248,000.00
5	2021	Due 365 days from Year 4 payment	\$248,000.00



## Pricing

Reference Exhibit C for Pricing breakout

## Contract Sum

Securus' systems and services provide a complete solution that includes deploying a project team, customizing and configuring the SECURUS system for CCD's use, managing change, completing integration with SECURUS into existing CCD systems, performing data migration tasks, hosting the solution, coordinating all initial and on-going customized product/procedure training, and providing feature enhancements, maintenance and support for the product.

## 14 Service Levels

Securus agrees to repair and maintain the System in good operating condition (ordinary wear and tear excepted), including, without limitation, furnishing all parts and labor. All such maintenance shall be conducted in accordance with the service levels in Items 1 through 10 below. All such maintenance shall be provided at Securus' sole cost and expense unless necessitated by any misuse of, or destruction, damage, or vandalism to any premises equipment by DSD (not inmates at the Facilities), in which case, Securus may recoup the cost of such repair and maintenance through direct invoicing, at Securus' option. DSD agree to promptly notify us in writing after discovering any misuse of, or destruction, damage, or vandalism to, the said equipment. If any portion of the System is interfaced with other devices or software owned or used by DSD or a third party, then Securus shall have no obligation to repair or maintain such other devices or software. This service level agreement does not apply to any provided Openworkstation(s) (see below). For the services contemplated hereunder, Securus may provide, based upon the facilities requirements, two types of workstations (personal computer/desktop/laptop/terminal): The "Openworkstation" is an open non-secured workstation which permits administrative user rights for facility personnel and allows the facilities an ability to add additional third-party software. Ownership of the Openworkstation is transferred to the facility along with a three-year product support plan with the hardware provider. Securus has no obligation to provide any technical and field support services for an Openworkstation. DSD is solely responsible for the maintenance of any Openworkstation(s)."

**Service and Support**

Securus shall provide highly reliable service from initial system design and installation through ongoing maintenance and support. The service and maintenance program should include integrated remote programming, diagnostics, downloading, and troubleshooting capabilities. Securus does not charge for maintenance, support, training, and repair of system software and equipment. The local Securus service and account management team will provide support 24 hours per day, seven days per week, and 365 days per year (24x7x365).

**Outage Report -Technical Support**

If either of the following occurs: (a) DSD experience a System outage or malfunction or (b) the System requires maintenance (each a "System Event"), then DSD will promptly report the System Event to Securus Technical Support Department ("Technical Support"). DSD may contact Technical Support 24 hours a day, seven days a week (except in the event of planned or emergency outages) by telephone at 866-558-2323, by email at TechnicalSupport@securustech.net, or by facsimile at 800-368-3168. Securus will provide DSD commercially reasonable notice, when practical, before any Technical Support outage.

**Priority Classifications.**

Upon receipt of DSD report of a System Event, Technical Support will classify the System Event as one of the following three priority levels:

"Priority 1"	30% or more of the functionality of the System is adversely affected by the System Event.
"Priority 2"	5% - 29% of the functionality of the System is adversely affected by the System Event.
"Priority 3"	5% or less of the functionality of the System is adversely affected by the System Event. Single and multiple phones related issues.

**Response Times**

After receipt of notice of the System Event, Securus will respond to the System Event within the following time periods:

Priority 1	2 hours
Priority 2	24 hours
Priority 3	72 hours

### Response Process

In the event of a System Event, where the equipment is located on Customer premises. Technical Support will either initiate remote diagnosis and correction of the System Event or dispatch a field technician to the Facility (in which case the applicable regional dispatcher will contact DSD with the technician's estimated time of arrival), as necessary. In the event a System Event occurs in the centralized SCP system; technical support will initiate remote diagnosis and correction of the System Event.

### Performance of Service

All of Securus' repair and maintenance of the System will be done in a good and workmanlike manner at no cost to DSD except as may be otherwise set forth in the Agreement. Any requested modification or upgrade to the System that is agreed upon by DSD and Securus may be subject to a charge as set forth in the Agreement and will be implemented within the period agreed by the parties.

### Escalation Contacts

DSD account will be monitored by the applicable Territory Manager and Regional Service Manager. In addition, DSD may use the following escalation list if Securus' response time exceeds 36 hours: first to the Technical Support Manager or Regional Service Manager, as applicable, then to the Director of Field Services, then to the Executive Director, Service.

### Notice of Resolution

After receiving internal notification that a Priority 1 System Event has been resolved, a technician will contact DSD to confirm resolution. For a Priority 2 or 3 System Event, a member of Securus' customer satisfaction team will confirm resolution.

### Monitoring.

Securus will monitor Securus back office and validation systems 24 hours a day, seven days a week.

### Required IGR.

DSD is responsible for providing a dedicated isolated grounded receptacle ("IGR") for use about the primary System. Upon request, Securus will provide DSD with the specifications for the IGR. If DSD is unable to or do not provide the IGR, then Securus will provide the IGR on a time and materials basis at the installer's then-current billing rates, if Securus is not responsible for any delay caused by DSD's failure to provide the IGR.



### End-User Billing Services and Customer Care.

Securus Correctional Billing Services department will maintain dedicated customer service representatives to handle end-user issues such as call blocking or unblocking and setting up end-user payment accounts. The customer service representatives will be available 24 hours a day, 7 days a week by telephone at 800-844-6591, via chat by visiting Securus' website [www.securustech.net](http://www.securustech.net), and by facsimile at 972-277-0714. In addition, Securus will maintain an automated inquiry system on a toll-free customer service phone line that will be available to end-users 24 hours a day, 7 days a week to provide basic information and handle most routine activities. Securus will also accept payments from end-users by credit card, check, and cash deposit (such as by money order, MoneyGram or Western Union transfer).

### Jail Working Conditions

Securus shall follow the Denver Sheriff Department rules and regulations working within the jail for the safety and security of inmates, staff and vendors. This will include, but not limited to;

- A criminal record background check being conducted on all new employees, contractors, and volunteers prior to their assuming duties to identify whether there are criminal convictions that have a specific relationship to job performance.
- Tool Inventory upon entrance and exit of facility.
- Prior coordination and approval through Project Manager of any onsite work. Work shall be detailed out.

More comprehensive rules and regulations for tools and personnel will be provided to the vendor. The Denver Sheriff's Department will provide a reasonable location for the storage of materials and tools.

Appendix A: Cloud Requests (See attached)

Securus shall comply with attached "Securus VV Cloud Requests.pdf" as responded and agreed to within the RFP

---

Appendix B: Business Requirements (See Attached)

Securus Video Visitation terminals and visit stations comply with all ADA requirements.

**3 – Construction and Installation**

3.1 The vendor shall furnish, install and maintain video visitation equipment, hardware, software and network components.

3.2 The vendor shall furnish all necessary labor, tools, equipment and supplies related to completing the installation of the solution.

3.3 The vendor shall be responsible for obtaining any and all permits and inspections (including the cost thereof) that are required by government authorities to complete installation of the solution.

3.4 The vendor shall clearly, logically and permanently mark all components of the system so that they can be easily identified by the City. Components may include, but are not limited to, switches, connectors, jacks, receptacles, outlets, cables and cable terminations.

3.5 The installation shall be in compliance with the City of Denver Building and Fire Codes.

3.6 The vendor shall be responsible for performing all equipment and system testing, adjustments as necessary to ensure system functionality.

*Response SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

As demonstrated with the installation and implementation of the City's existing ITS solution, Securus will provide all necessary labor, tools, equipment and supplies to complete the construction and installation of our solution, and comply with all testing requirements, City building and fire codes.

**4 – Storage, Data Retention, Backup and Recovery**

4.1 Video Playback - The solution shall allow playback of video recorded visits on an unlimited number of user PC's throughout DSD.

4.2 Data Retention:

a. Visit Records: Visit records shall be retained indefinitely, even after an inmate has been released, so that a complete visit history is maintained for inmates over multiple bookings.

b. Video:

Video recordings of social visits shall be retained for 90 calendar days.

The system shall have functionality to allow designated DSD staff to place a lock on a selected video recording to prevent it from being purged after the standard retention period.

c. The system shall not automatically delete any records in bulk at any time.

**SECURUS HAS READ, UNDERSTANDS AND COMPLIES**

Standard video recording retention is 30 days; however Securus will retain the DSD's recordings for 90 calendar days. Our system will have functionality to allow designated DSD staff to place a lock on a selected video recording to prevent it from being purged after the standard retention period.

4.3 Backup and Disaster Recovery

a. For locally hosted solutions, the vendor shall work with the City to develop a Business Continuity Disaster Recovery plan that meets the City's disaster recovery needs.

b. For vendor-hosted solutions, the vendor shall perform daily incremental backups and full backups at least weekly.

*Response: SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

**5 – System Hardware**

5.1 Locally hosted solutions, or any on-premises components of the solution, shall be installed on the City's hardware and must be able to function in accordance with the City's approved operating system standards. Refer to – EA Technology Standards.

*Response SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

**6 – Solution Architecture**

6.1 Open Architecture - The solution shall have an open architecture for all equipment and software to provide flexibility in upgrading and replacing individual software or hardware components in the future.

6.2 Operating System - Locally hosted solutions shall be able to function in accordance with the City's approved operating system standards. Refer to Exhibit 5 – EA Technology Standards.

6.3 Databases - Locally hosted solutions shall be compatible with the City's database requirements. Refer to Exhibit 5 – EA Technology Standards

6.4 Scalability - The proposed system shall be scalable to support future user demand and potential system interfaces.

*Response : SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

## **7 – Integrations**

7.1 The video visitation system shall be integrated with DSD's Jail Management System (JMS) so that relevant inmate information from JMS can be integrated with the solution's scheduling functionality. Note that plans to replace the existing JMS in 2017, therefore an integration will not be pursued until the new JMS is in place.

*Response: SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

## **8 – Data Migration**

8.1 The vendor of the replacement solution shall migrate all existing visit records - including social and professional visits - that currently reside in DSD's Jail Management System (JMS) into the new solution so that each inmate's complete visit history can be accessed from a single application. The current data load of visit records in the JMS consists of approximately 30 MBs for roughly 240,000 visit records. Video recorded visits will not be migrated into the new solution as the retention period is only 90 days.

*SECURUS HAS READ, UNDERSTANDS AND COMPLIES*

## **9 – Security**

9.1 Authentication and Role Based Permissions - The system shall utilize a directory service that can assign role-based permissions in order to access and view specific features based on job title, department, etc.

9.2 User Administration - The system shall allow City staff members who are assigned system administrator rights, to grant access, assign and change roles for system users.

9.3 Audit Trail - The system shall record a detailed log of all activity performed within the application such as administrative tasks and source and destination IPs of the facility visitation terminals and home internet connections for remote visitation, etc.

9.4 Cloud Security - For vendor-hosted solutions, the solution shall meet the City's security standards as outlined in Exhibit 3 – Cloud Services Requirements.

**SECURUS HAS READ, UNDERSTANDS AND COMPLIES**

SVV provides the City with the most advanced features for authentication, user administration, and other security features as requested. The following screen shows the configurable options available to the User Profiles. Agencies normally limit the Administrator Role to one or two people. This helps to control who can or cannot create new users, expand user's capabilities, change agency visitation policy (phone schedules), and add, change, or delete security templates.

**10 – System Availability**

10.1 The solution shall be highly available where the system is available 24 hours/day, 7 days/week, 365 days/year. Both facilities permit visits on weekends and evenings and professional visits are permitted 24 hours/day, 7 days/week.

10.2 Planned Maintenance - There shall be no more than 4 hours of downtime per month for planned maintenance. Downtime shall be scheduled outside of facility social visit hours only and the vendor shall notify the appropriate City staff a minimum of one week in advance.

**SECURUS HAS READ, UNDERSTANDS AND COMPLIES**

The City will continue to be supported by our state-of-the-art Network Operations Center in place for the ITS solution. Our Network Operations Center (NOC) is dedicated to monitoring and measuring the performance of SVV. When outages occur, our NOC staff handles them quickly to limit customer impact to total system failure.

The following statistics show the SVV uptime for 2014:

SVV User Interface Availability = 99.987% uptime

SVV Platform Availability = 99.987% uptime

SVV Network Availability = 100% uptime.

The following statistics show the SVV uptime for 2015:

SVV User Interface Availability = 99.870% uptime

SVV Platform Availability = 99.870% uptime

SVV Network Availability = 99.885% uptime.

**B.9 DSD VISIT POLICY AND CURRENT PROCESS OVERVIEW:**

Both DSD detention facilities permit social and professional visits.

**B.9.a Social Visits**

Social visits must be scheduled in advance for both facilities; however, social visits are permitted on a walk-in basis at DDC for inmates housed on the 2nd floor (excluding Pod 2D). DSD has one full-time Visit Reservationist that manages scheduling for both facilities, which is currently a manual process as the existing visit systems at both jails do not include scheduling modules. The Visit Reservationist manually enters visit information into the inmate's record in JMS when the reservation is made.

*Visit Eligibility* – Social visit privileges are based on the following:

- Time in (COJL only) – The inmate must have been in the facility a minimum of 10 days. If the inmate was transferred from DDC to COJL, the time at DDC does not count toward the 10 days.
- Housing location – Inmates housed in certain areas of the jail (e.g. special management) may not be eligible for social visits.
- Visit privileges haven't been revoked.
- Visit quotas E.g. Two visits per weekend (visit limits may vary by housing location).

*Video Recorded Visits* – Social visits at DDC are automatically video recorded, saved and available for playback by designated DSD personnel, including Gang Unit Investigators and Internal Affairs. The existing visit system at COJL does not have functionality to video record visits.

*Visit Quotas* – Inmates are permitted a limited number of social visits in a given week:

- COJL: 2/week, which may consist of 2 single visits or 1 single and 1 group/family visit. The two visits may not be scheduled on the same day. Work Release inmates (Buildings 19 and 24) are permitted 1/week.
- DDC:
  - Walk-in visits: 1/day
  - Scheduled social visits: 2/week, which may be either 2 single visits or 1 single and 1 group/family visit. The two visits may not be scheduled on the same day.

#### B.9.b Professional Visits

Professional visits are permitted on a walk-in basis only, 24 hours/day, 7 days/week at both facilities. With the exception of the inmate's attorney, professionals who wish to visit an inmate must obtain permission in advance. The respective jail's Operations team is responsible for processing requests, and permission is typically granted in six-month increments. A separate request is required for each inmate to be visited. All professional visits are conducted in person and not via the video visitation system.

#### B.9.c Visit Tracking and Record Retention

Inmate visit history, including social and professional visits, is tracked in DSD's JMS since the existing visitation systems at both jails lack functionality to do so. Each visit is manually entered directly into JMS as it is not interfaced with either visitation system. Visit records are retained indefinitely, even after an inmate has been released, so that a complete visit history is available over multiple bookings.

**B.9.d Visit Policy Summary Table**

	Social Visits		Professional Visits
	DCJ	DDC	DCJ & DDC
Reservation Required?	Yes - All visits	Yes - For inmates on floors 3 - 5 and Pod 2D	No - Walk-ins only
Visit Hours Scheduled Visits	<ul style="list-style-type: none"> <li>▪ Fri - Sun Weekly</li> <li>▪ Noon - 8:00 p.m.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Daily</li> <li>▪ 7:00, 8:00, 9:00 a.m. or 6:00, 7:00, 8:00 p.m.</li> </ul>	N/A
Walk-in Visits Permitted?	Not permitted	Permitted for inmates housed on 2 <sup>nd</sup> floor, except Pod 2D	All professional visits conducted on a walk-in basis only.*
Visit Hours Walk-In Visits	N/A	<ul style="list-style-type: none"> <li>▪ Daily</li> <li>▪ 7:00 - 9:00 a.m., Noon - 2:00 p.m. and 6:00 - 8:00 p.m. (first come, first served)</li> </ul>	24 hours/day, 7 days/week
Video or In Person?	Via video system	Via video system	In person
Visit Duration	30 minutes	30 minutes	N/A
Visit Quota	2/week (no more than 1 in a single day), except Buildings 19 and 24 (work release) 1/week	<ul style="list-style-type: none"> <li>▪ Walk-in visits: 1/day</li> <li>▪ Scheduled visits: 2/week (no more than 1 in a single day)</li> </ul>	None

*\* With the exception of the inmate's attorney, professional visitors must obtain approval to visit a specific inmate from the facility's Operations team, which is typically granted for a six-month period.*

**SECURUS HAS READ AND UNDERSTANDS**

**B.10 BUSINESS USERS:**

There will be a total of approximately 50-60 DSD staff members from the following areas that will use the system:

- Scheduling
- COJL Operations, Classification and Officers
- DDC Operations, Classification and Officers
- DSD Gang Unit Investigations
- DSD Internal Affairs

*Response: SECURUS HAS READ AND UNDERSTANDS*



**B.11 VISIT VOLUMES:**

An estimated 30,000+ social visits and 17,000+ professional visits are completed across the two jails annually, with social visits making up about 2/3 of the total volume.

*Response: SECURUS HAS READ AND UNDERSTANDS*

**B.12 BUSINESS RULES: INMATE VISITS (SOCIAL AND PROFESSIONAL VISITS):**

The following are the business rules for DSD's current process for both social and professional visits. These rules dictate the process constraints and conditions that the solution must be able to operate within.

1. Social Visits		
ID	Name	Rule
1.1	Facility visit hours	<p>Visit days and hours vary by facility and also by housing location within each facility:</p> <p><b>DCJ:</b></p> <ul style="list-style-type: none"> <li><i>Scheduled visits only, no walk-ins. 3 days/week: Friday - Sunday (buildings 19 &amp; 24 Saturday and Sunday only), 52 weeks/year.</i></li> <li><i>Visits are not scheduled for holidays that fall outside of the normal Friday – Sunday visit days.</i></li> </ul> <p><b>DDC:</b></p> <ul style="list-style-type: none"> <li><i>Scheduled visits: 7 days/week, 52 weeks/year.</i></li> <li><i>Walk-in visits: 7 days/week, 52 weeks/year (permitted only for inmates housed on the 2<sup>nd</sup> floor with the exception of Pod 2D, which requires scheduled visits).</i></li> </ul>
1.2	Time-In Requirement (DCJ only)	Inmates at DCJ must have been in the facility a minimum of 10 days to qualify for social visits. If the inmate was transferred from DDC to DCJ, the time in DDC does not count toward the 10 days.
1.3	Visit Privileges	<p>Inmates who have lost visit privileges are not permitted any social visits.</p> <p>When an inmate loses visit privileges, any social visits that have already been scheduled will be cancelled.</p>
1.4	Non-Association Orders	If a non-association order in place between two inmates, the inmates may not be scheduled for visits at the same time.
1.5	Visit Quotas	<p>Inmates are permitted a limited number of social visits during a specified period of time. Quotas vary by housing location:</p> <p><b>DCJ:</b></p> <ul style="list-style-type: none"> <li>- Buildings 1, 4, 21, 22 – Inmates are allowed 2 visits/week. The two visits may be either 2 single visits or 1 single and 1 group/family visit (2 group visits not permitted). The two visits may not be scheduled on the same day.</li> <li>- Buildings 19 and 24 (community</li> </ul>

1. Social Visits		
ID	Name	Rule
		<p>corrections/work release) – 1 visit per week.</p> <p><b>DDC:</b></p> <ul style="list-style-type: none"> <li>- <i>Walk-in visits:</i> 1 per day</li> <li>- <i>Scheduled social visits:</i> Inmates are allowed two visits/week, which may be either 2 single visits or 1 single and 1 group/family visit. The two visits may not be scheduled on the same day.</li> </ul> <p>Scheduled visits where the visitor was a “no show” are still counted toward the inmate’s visit quota.</p>
1.6	Visitor Information	<p>The following information for each visitor is entered into the visit record:</p> <ul style="list-style-type: none"> <li>a. Full name (including middle name or middle initial)</li> <li>b. Date of birth</li> <li>c. Government issued ID # (e.g. driver’s license, passport, state issued license, military ID, etc.)</li> <li>d. Relation to inmate</li> <li>e. Phone number</li> <li>f. Email address</li> </ul>
1.7	Advance Scheduling	<p>Scheduled visits may be scheduled no less than 7 days in advance of the date requested (and are typically not scheduled out longer than a week due to the frequency that inmates change housing locations).</p>
1.8	Individual vs. Group Visits	<ul style="list-style-type: none"> <li>• Individual visit – 1 visitor only</li> <li>• Group/family visit – 2 or more visitors with a maximum of 3 allowed, including infants and children.</li> </ul>
1.9	Scheduled Visits – Visitor Name	<p>For visits scheduled in advance, the name of each visitor must be listed on the visit reservation and only those listed may participate in the visit. No substitutions are allowed.</p>
1.10	Criminal Background Check	<p>For all scheduled visits at DCJ, DSD’s NCIC department completes a criminal background check on all visitors, and the inmate, to check for:</p> <ul style="list-style-type: none"> <li>• Protective orders that would prohibit contact between the visitor and the inmate.</li> <li>• Active arrest warrants on the visitor.</li> </ul> <p>If a protection order is in place, the visit will be cancelled unless the visitor can produce court documents showing the order is no longer active or that the protection order allows jail visits.</p> <p>Designated facility corrections officers are notified about any</p>



# Program Management Office Scope of Work

<b>1. Social Visits</b>		
<b>ID</b>	<b>Name</b>	<b>Rule</b>
		visitors that have active warrants and the scheduled visit date.
1.11	Visit Check-In	Visitors are required to check in at the Information Desk in the facility's lobby 30 minutes prior to the visit start time.
1.12	Visitor ID	Each visitor must show a valid government issued ID such as driver's license, state issued ID, military ID, consulate ID or passport.  If a visitor is 16 or 17 years of age and does not have a government issued ID, they are asked to provide a school ID if they have one.
1.13	Visit Record	The following information is entered (for each visitor) with the visit record: <ul style="list-style-type: none"> <li>• Visit Date</li> <li>• Visit Time</li> <li>• Visitor(s) Name</li> <li>• DOB</li> <li>• Valid ID #</li> <li>• Relation to inmate</li> </ul>
1.14	Walk-In Visits	DDC: Walk-in visits are granted on a first come, first served basis. Once the Information Desk Officer has determined that the inmate qualifies for a visit, the visitor will be checked in and instructed to take a number and will be called when a visit kiosk is available.  DCJ: All social visits at DCJ are scheduled in advance. Only those who have traveled more than 200 miles will be permitted to visit on a walk-in basis. ID and proof of travel is required.
1.15	Visit Start Time and Duration	All visits start at either the top of or at half past each hour and are 30 minutes in length.
1.16	Visit Disposition	The final outcome of each visit (completed, canceled, no show) is recorded with the visit record.
1.17	Visit History and Retention – Visit Records	A record of all visits including completed, cancelled and no-shows, are retained with the inmate's file.  Retention: Visit records are retained indefinitely even after the inmate has been released or transferred out of DSD's detention facilities.
1.18	Visit History and Retention – Video Recordings	DDC: A video recording of all social visits at DDC are retained and available for playback by designated DSD personnel such as Gang Unit Investigators and Internal



# Program Management Office Scope of Work

1. Social Visits		
ID	Name	Rule
		<p>Affairs.</p> <p>DCJ: The current visit system at DCJ does not have functionality to video record visits, however, social visits at this facility will be video recorded when the new visit system is in place.</p> <p>Retention: There is currently no official retention for the video recordings, however, DSD will likely retain video recordings for 90-days when the new visit system is in place.</p>

2.0 Professional Visits		
ID	Name	Rule
2.1	Visit Hours	Professional visits are permitted on a walk-in basis only, 24 hours/day, 7 days/week, 52 weeks/year at both facilities.
2.2	Advance Permission	<p>With the exception of the inmate's attorney and law enforcement personnel, professionals who wish to visit an inmate are required to obtain permission in advance. The respective jail's Operations team is responsible for processing requests, and permission is typically granted in six-month increments.</p> <p>A separate request is required for each inmate to be visited.</p>
2.3	Visit Check-In	<p>Professional visitors are required to check in at the Information Desk in the facility's lobby and must present a copy of the approved request and a valid ID.</p> <p>The visitor must then complete an <i>Official Visit Request</i> form. The Information Desk Officer adds the names of all persons who are in the visit party to the <i>Official Visitor Log</i>, along with time in and time out, so they know who is in the jail at any given time.</p>
2.4	# of Visitors	There may be more than one person in the visiting party as long as each person has obtained permission to visit the inmate in advance.
2.5	In-Person Visits	Professional visits are conducted in person and not via the video visit system.

<b>2.0 Professional Visits</b>		
<b>ID</b>	<b>Name</b>	<b>Rule</b>
2.6	Visitor Information	<p>The following information for each visitor is entered into the visit record:</p> <ul style="list-style-type: none"> <li>• Visitor Name</li> <li>• Occupation (e.g. attorney, clergy, police, etc.)</li> <li>• Valid ID #</li> <li>• DOB</li> <li>• Phone</li> </ul>
2.7	Visit Quotas	There is no limit on the number of professional visits an inmate may have in a given period of time.
2.8	Visit History and Retention	A record of all professional visits are retained indefinitely with the inmate's file, even after the inmate has been released or transferred out of DSD's detention facilities.

**SECURUS HAS READ, UNDERSTANDS AND COMPLIES**

**B.13 CONSTRUCTION AND REMODELING CONTRACTING PROVISIONS:**

Vendor shall be responsible for obtaining any and all permits (including the cost thereof) required to perform this installation. The installation shall be in complete compliance with City of Denver Building and Fire Codes.

**SECURUS HAS READ, UNDERSTANDS AND COMPLIES**

## Appendix D: Preliminary Implementation Plan

### *Denver Sheriff Department Preliminary Implementation Plan*

#### *1.0 Implementation Team Commitment and Confirmation of Understanding*

Securus Technologies has a proven track record of providing successful turnkey installations for large County and State Departments of Corrections, as demonstrated by our on-time previous installations with the City and our track record throughout the United States.

Each of these video implementations present similar challenges as other installation items. Due to Securus' expertise and business acumen, Securus has already developed a proven transition process and associated procedures that will facilitate the transfer of existing inmate data element listings and other critical system hardware and system products and features.

Based upon our past experiences, installing these very similar installations, Securus fully commits to the City's requested install time frame of ninety (90) calendar days. As an added value to the City, not only will Securus install the Phase 1 facilities within ninety (90) calendar days, we will also complete installation of the all facilities during this time frame.

As further demonstration of our commitment to meet the requested installation time frame, Securus will assign a minimum of 3 installation technicians dedicated to the City installation. These technicians are in addition to the assigned account team, install management and centralized support teams that will be focused on the City installation and transition.

Within the pages to follow, Securus has provided our proposed Preliminary Implementation Plan (The Plan). The Plan provides details regarding our overall approach to the implementation and transition of the SCP Inmate Video Service for the City. Details include our proposed phase and regional installation approach, facility assignments by regional, installation team assignments, long term account management and site technician plan, key dates, quality control check points and finally a Gantt chart showing our proposed installation schedule by facility.

The time frames and offered schedules are based upon what we know today about the City's facilities and our past experience in installing multi-location, statewide State Departments of Corrections. Upon contract award, Securus will meet with the City (City Team) to refine and finalize the overall plan and schedule. We fully expect to make adjustments to this plan based upon the City Team's valuable input.

Our Project Management Organization is comprised of Project Management Professionals and seasoned Installation Technicians with multiple years successfully working in a corrections environment and completing complex, multi-location state installations. Securus as well as all installation team members fully understand that the SVV will be deployed in facilities within a custodial/secured environment and therefore certain security and operational requirements are enforced. Securus has reviewed, understands and accepts the City access and rules. Securus as the sole contractor further understands and accepts the following:

- Installation activities shall be accomplished during the hours of 6:00a.m to 5:00p.m Monday through Friday or as specified by each facilities.

- Friday's shall be utilized for SVV testing and/or training of City staff.
- Securus will be responsible for clean-up and remove all trash and packaging materials resulting from work performed. Unless otherwise specified by City, no equipment, inventory or spare parts shall be stored by Securus at the Facilities.
- Securus will be responsible for correction of any damage to City's property caused by maintenance or installation associated with the SVV, including repairs to walls, ceilings, etc.
- Install of equipment will be in accordance with City's requirements.
- Securus shall work with City to address any environmental conditions identified in a City Facility phone room and our implementation plan will account for any changes that need to be made based upon our initial implementation site surveys. Securus further understands that any phone room changes required will be performed at no cost to the City.
- Securus will obtain City's written approval before making any physical changes to the Facilities, such as drilling into walls, floors, ceilings or any other portion of the Facilities to include existing, newly constructed and/or expanded Facilities.
- Securus may, at SVV own risk, utilize existing SVV conduit, raceways, cable, wiring, switches and terminals within the Facilities. If during the term of the subsequent Contract, any existing network wiring needs to be repaired or replaced; Securus shall repair and/or replace such network wiring at no cost to City.
- Exposed network wiring is not permitted and that the use of external conduit shall be approved by City with each installation.
- Securus understands and accepts that existing network wiring concerns identified for the following Facilities and that corrections will be made at Securus' expense:
  - Securus understands that additional wiring issues may exist but are unknown to the City at this time.
  - Securus agrees that if any cabling work is required as part of any installation, all new cables shall be used and marked clearly and legibly at both ends, and meet all applicable Electronic Industries wiring standards for commercial buildings and must be approved by the Facilities' maintenance personnel.
  - Securus shall install, repair and maintain all Contractor-provided equipment and lines, including but not limited to, any wiring or cable work required from the demarcation throughout the Facilities. All Securus-provided equipment, installation, maintenance, repair costs and all costs or losses due to vandalism shall be the total responsibility of Securus.
  - Securus shall provide written documentation indicating that all circuits have been tested and all cables, pairs, fiber strands, blocks, etc. are legibly marked after the completion of each installation.

- Securus shall provide, install, maintain, replace and upgrade adequate surge and lightning protection on all equipment used for the SVV.

Independent of our Project Management Organization, the Securus Implementation Services Team performs frequent quality audits and timely customer satisfaction surveys to ensure the voice of the customer is always heard. Over the last 6 years and 2,200 SCP installations, the Securus Project Team has averaged a 4.6 (out of 5) Customer Satisfaction rating. Our industry leading experience combined with our rigorous focus on quality and customer feedback has resulted in a finely tuned installation process that delivers on our commitments and ensures customer satisfaction.

## *2.0 Transition Plan Development and Initiation*

### 2.1 Transition Initiation

Immediately upon contract signature, Securus will distribute the listing of Points of Contact (POC) for each of the City facilities provided in the RFP. Securus will request a Kick-off meeting with the City Team so that we may present and review in detail our proposed Preliminary Plan. Securus fully expects to make adjustments to the Plan based upon the City Team's input. Upon completion of the meeting, Securus will finalize and submit the updated Plan, within five (5) business days, to the Primary City Team member for review and approval. Securus understands and accepts that the resulting approved Plan will become part of the SVV Contract between Securus and the City. Securus further understands that the 120 calendar day implementation time frame will begin 10 business days following approval of the final Plan.

### 2.2 Kick-off Transition Plan Meeting

As stated above, Securus will request a Kick-off Transition Plan meeting to be held with the City Team directly following contract signature. This meeting will be critical in the review and development of the Final Transition Plan to be submitted to the POCs for review and approval. The Kick-off meeting will include review of the proposed phase/regional approach and site cutover schedule as well as discussion on each of the following topics all of which will be detailed within the Final Transition Plan.

- Review, approval and/or adjustment of Phase and Regional Assignments
- Review, approval and/or adjustment of Proposed Transition Schedules
- Finalized Customer Requirements document
- Approved Scope Statement
- Work Breakdown Structure
- Critical Milestones and order of Milestones
- Quality Plan
- Communications/Reporting Plan
- Risk Management/Contingency Plan
- User and City Web Based Interface
- Calling Rates and Fees Confirmation

- Inmate PIN Transfer from existing vendor
- Inmate PAN listing transfer from existing vendor
- PIN Management Processes
- PAN Management Processes
- Calling Options Feature and Functionality
- CITY Systems Integration (Inmate Paid Debit, Commissary Order etc.)
- Proposed Site Technician Assignment and Management Plan
- Administrative Staff Hiring and Location Assignments
- Overall Site Transition Schedule

The following Securus Personnel, at a minimum will be on-site during the Kick-off meeting:

- Major Account Manager
- Implementation Supervisor
- Implementation Project Manager
- In-state Technicians
- Installation Technicians

### 2.3 Plan Implementation

Upon completion of the Kick-off meeting, Securus will submit the updated Plan, within five (5) business days, to the POCs for review and approval. Immediately upon approval, the Plan will be implemented for all approved sites.

Securus will follow the procedures as detailed within the document and refined based upon City input, to complete an on-time transition of all systems, hiring of all on-site personnel and training of all system users.

### 2.4 Project Execution

During Project Execution, Securus Technicians will travel to each location and complete pre-installation activities in preparation for the SCP SVV cut-over. The pre-installation activities include pre-wiring, hardware staging, and telecom test & turn-up activities that can be done in advance to reduce the amount of time and complexity of the actual cut-over.

The Securus Project Management Team will coordinate cut-over activities with the City Team and the current services provider to ensure a seamless transition of phone service. Transition of service can be coordinated for after hours or during inmate lockdown to limit service interruptions. If a service interruption is required, the activity will be coordinated with the City Team at least 5 business days in advance of the scheduled activity and schedules can be adjusted to meet the needs of the City sites. During the cut-over, the Securus Team will perform a thorough inspection of the installation and will resolve any potential issues prior to finalizing the implementation.

The technicians completing the installation activity will perform a walk-through with the City Team to review all installation documentation and checklists. The Securus Project Management Team will host a Customer Acceptance Review Meeting with the City Team and each site prior to finalizing the each individual site cut-over.

Onsite training seminars as well as web-based training activities (if applicable) will occur during this phase of the project to include on-site training personnel at each site on the day of cutover.

Weekly implementation meetings and Project Team "Touch Point" meetings will occur as part of Project Execution. These meetings will allow both Securus and the City Team to closely evaluate project activities and provide bidirectional feedback regarding project performance.

### 2.5 Transition Closure

During the Transition Closure Phase, the Securus Implementation Management Team will ensure there are no outstanding actions or deliverables, and will work with the City POC Team to review the complete transition and obtain City acceptance.

The Securus Implementation Management Team will transition support responsibilities to the Securus Account Management Team for long-term ongoing account support. The Securus Implementation Management Team will complete all internal updates and implementation closure activities.

## 3.0 Program Management

### 3.1 Transition Oversight Authority

The Securus Implementation Team (Field Services and Installation/Site Engineering Support) reports to the Sr. Director of Installation & Field Operations. The Transition is supported by Executive level sponsorship, represented by the Vice President of Service & Technical Operations, Mr. Danny deHoyos and our Executive Vice President of Sales, Mr. Josh Conklin and the Vice President of DOC Sales, Mr. Matt Anderson.

The Securus Implementation Team, including our internal Implementation sponsorship and oversight authority, will serve as primary executing agency and have direct control and accountability for all personnel used to complete the Implementation.

The assigned Securus City Major Account Manager, will serve as an oversight authority on behalf of the customer agency. There will be a partnership between the assigned Securus City Team and the City Team to ensure the Transition is completed as planned and all events occur on time.

The table to follow shows each team member and their responsibilities.

<b>Role</b>	<b>Responsibility</b>
<b>Regional Implementation Team Lead</b>	<ul style="list-style-type: none"> <li>Coordinate Implementation Initiation Phase</li> <li>Review and finalize Implementation plans</li> <li>Monitor Implementation activity, and complete Implementation/task audits.</li> <li>Perform quality reviews and customer satisfaction follow-up</li> <li>Escalation assistance</li> </ul>
<b>Implementation Manager</b>	<ul style="list-style-type: none"> <li>Primary point of contact for the City</li> <li>Material and human resource coordination</li> <li>Telecom coordination and delivery</li> <li>Transition coordination w/current inmate services provider</li> <li>Customer communications</li> <li>Implementation Plan management</li> </ul>
<b>Implementation Coordinator</b>	<ul style="list-style-type: none"> <li>Order follow-up</li> <li>Task management and updates</li> <li>Assist Implementation Manager as required</li> </ul>
<b>Installation Technical Support</b>	<ul style="list-style-type: none"> <li>Provisions Securus SVV for customer specific requirements.</li> <li>Provides support for Field Service Technicians</li> <li>Data uploads (PIN/PAN/Block, Privileged numbers)</li> </ul>
<b>Site Engineering</b>	<ul style="list-style-type: none"> <li>Detailed site schematics and provisioning plans</li> <li>Materials and telecom requirements analysis</li> <li>Implementation support</li> <li>Post-Implementation monitoring and analysis</li> </ul>
<b>Field Service Technician(s)</b>	<ul style="list-style-type: none"> <li>On-Site equipment installation and configuration</li> <li>Telecom test &amp; turn-up activities</li> <li>On-Site quality checklists and customer reviews</li> </ul>

Role	Responsibility
<b>Installation &amp; Engineering Manager</b>	Implementation activity oversight Implementation Team management and quality reviews Customer communications Escalation Support
<b>Regional Field Service Manager</b>	Field service & Installation Team support Human resources coordination Customer communications On-Site quality evaluations Escalation Support
<b>Major Account Manager</b>	Internal Implementation oversight Customer communications Customer account management Escalation Support
<b>Quality Assurance Technician</b>	Customer provisioning and engineering quality control reviews Quality assurance management and data reporting
<b>Implementation Management QA Analyst</b>	Customer Satisfaction survey and communication activities Implementation Management quality reviews and task monitoring Quality assurance management and data reporting

### 3.2 Installation Team Staffing and Regional/Phase Approach

#### **Field Installation Team:**

Securus will make every effort to limit the administrative burden that can occur during a transition of service providers. We have the experience of installing our SCP in over 2,200 customer locations. This level of experience ensures that we do not waste any of your time. Our teams arrive at your facilities ready to get the job done and prepared.

Securus has significant full time on staff installation technicians and will assign them to each of the install locations to be dedicated to the installation. All technicians are fully trained on the Securus SCP SVV and have significant experience with our technology.

Our expert Field Installation Team will be led by the Regional Field Services Managers and Field Services Specialists with oversight by the Project Manager. The Field Installation Team will be responsible for all on-site installation activities.

The regional installation teams will meet with each on-site City facility contract prior to start of the installation to review all steps of the process. These well-organized meetings will provide us with the opportunity to introduce the project members and review preliminary project plan and timetables with the local facility City contacts to ensure everyone is aware of the processes and procedures and can provide any site specific information that would be helpful in completing all tasks.

Our Project Managers will work with the City Team to coordinate equipment deliveries and facility access. When the Securus Technicians arrive onsite, they may require escorts to the phone and equipment locations. The majority of our project activity will occur during the install times of 6:00a.m and 5:00p.m Monday through Friday or as specified by the Facility. However, Securus Technologies can accommodate late-night/overnight cut-over activities. Some of our customers choose this method to eliminate service interruptions and we are more than comfortable supporting after hours cutovers. Fridays will be dedicated to testing and training.

During the Project Execution Phase, and if selected as an option for the City inmates, Securus Technicians will work with City Staff to organize schedules perform supervised terminal replacements for the detainees at each location for the deployment of the Securus video visitation (SVV) technology .

After each facility is transitioned to SVV, our Project Manager and Field Service Technician will review our quality checklists with the City Team.

Weekly stakeholder meetings will be hosted by the Securus Project Team and will involve participation from the City Team.

Once we identify the key personnel for the City Team we will input names in to our project schedule and provide a detailed activity list to all project participants.

**Phase and Facility Assignments:**

Typically, Securus will take a 2 Phase approach to the implementation and cutover of the City sites. Phase 1 will include all the terminal replacements at each location. Phase 2 will then include transition to the video activation. Due to the implementation requirements and to reduce down time, Securus will need to replace and turn up congruently throughout the facilities to reduce lost visitation scheduling. There will be some overlay of install preparations and circuit installation necessary to meet the 90 calendar day schedule. Securus commits that the installation activities performed at the facilities will in no way delay the visitations as best as possible. We can accomplish this because we have committed to providing dedicated full time installation technicians to the installation.

### 4.0 Transition Schedules

#### 4.1 Plan Milestones and Schedule

The following table provides a quick view of the Implementation milestones. The implementation team will complete this form with the aid of the City Team to insure compliance with City goals and objectives. Dates will be completed and provided to the City in the weekly meetings.

A Preliminary Implementation Schedule, in a Gantt format, has also been provided within this attachment. This schedule shows the preliminary listing of install activities by facility and the time frames assigned. This schedule will be adjusted following the kick-off meeting to meet the requirements and recommendations of the City Points of Contact.

Milestone	Planned Completion Date
<b>Implementation Kick-Off</b>	7/5/2016
<b>Site Inspections</b>	7/6/2016
<b>Initial Telecom &amp; Equipment Orders</b>	7/11/2016
<b>Final Implementation Plan Review &amp; Sign-off</b>	8/12/2016
<b>Pre-Installation Preparation / Customer provisioning completed</b>	8/4/2016
<b>LEC MPLS T1 Installations / LEC Delivery, Turn-up Prep</b>	8/22/2016
<b>Pre-Transition Installation Activities / Onsite wiring, equipment installation, Terminal replacements</b>	9/26/2016
<b>S-Gate User Interface Training / Onsite user training for City</b>	9/29/2016
<b>Implementation of Services</b>	10/3/2016

### 5.0 Program Control Plans

#### 5.1 Transition Monitor & Control

The Securus Implementation Team will coordinate cut-over activities with the City Team and the current services provider to ensure a seamless transition of phone service. Transition of SVV service can be

coordinated for after hours or during inmate lockdown to limit service interruptions. If a service interruption is required, the activity will be coordinated with the City Team at least 5 business days in advance of the scheduled activity and schedules can be adjusted to meet the needs of the City sites. During the cut-over, the Implementation Team will perform a thorough inspection of the installation and will resolve any potential issues prior to finalizing the implementation and transition. The technicians completing the installation activity will perform a walk-through with the City POC to review all installation documentation and checklists. The Securus Implementation Management Team will host a Customer Acceptance Review Meeting with the City Team and each site prior to finalizing the each individual site cut-over.

Onsite training seminars as well as web-based training activities (if applicable) will occur during this phase of the Implementation to include on-site training of personnel at each site on the day of cutover. Our finalized implementation schedule will provide additional information about the work packages and sequence of events that will occur during Implementation execution. The Securus Installation Team will work closely with the City to make sure our plan is 100% complete and fully accepted by the City Team prior to moving forward.

Weekly implementation meetings and Implementation Team "Touch Point" meetings will occur as part of the Implementation Execution. These meetings will allow both Securus and the City Team to closely evaluate Implementation and Transition activities and provide feedback regarding performance.

**Critical Implementation activities, such as Schedule Control, Quality Control, and Risk Control will be meticulously managed by our Implementation Management and Quality Assurance staff from the start of the implementation to the finish.**

All Installation Quality Control Checkpoints will be completed as part of the Implementation Monitor & Control processes. During the Implementation Monitoring/Controlling Phase, the Securus Implementation Management Team will focus on satisfying any outstanding action items. Additionally, the Securus Installation and Site Engineering Team will exercise daily diagnostic checks and monitoring protocols to ensure the recently installed equipment is working well and meeting the requirements of the City. During the Implementation Execution Phase, Securus Technicians will work with City Staff to perform supervised enrollments for the detainees at each Correctional Facility location.

## 5.2 Communication/Reporting Plan

At the beginning of the implementation, the Securus Implementation Management Team will work with the City Team to identify key stakeholders, additional points of contacts, and roles/responsibilities for the duration of the Implementation.

The Securus Implementation Management Team will establish regular meeting forums and communication protocols that accommodate the requirements of the City.

Throughout the duration of the implementation, our Implementation Management Team will provide weekly installation progress reports. The reports will include updates on all active, completed, and pending installation activities.

Once we've had the opportunity to meet directly with the City Team and establish meeting protocols and communication preferences, we will update and distribute the Implementation Communication Plan to all implementation participants.

## 5.3 Quality Control Plan

The Implementation Plan includes 5 Quality Control inspections at important stages throughout the implementation. The quality control inspections are essential elements of the implementation that ensure consistent high-quality work flows. The Securus Installation Support team utilizes a Six Sigma quality measurement technique, which identifies and removes the causes of errors, and minimizes variability in the installation process.

In total, our installation process has over 200 individual quality control points that are carefully reviewed and validated by our expert Technicians and Quality Assurance Analysts. Our current process sigma is 4.47, and our First Pass Quality rate is 94%. This means we execute the same high-quality processes every single time and if we do make an error, we do our best to catch it before it has a chance to create a problem. This attention to detail and level of focus on Implementation quality is truly unrivaled in our industry.

#### 5.3.1 Quality Control Checkpoint 1: Customer Provisioning

Prior to any onsite installation activity, the Securus Installation Support Technicians will provision the Securus SVV. The SVV provisioning activity prepares our system to support the City's inmate calling traffic, and ensures that all of the necessary applications and communication features are configured. After the customer provisioning is complete, the Installation Technician submits a quality control review form to the Engineer, Implementation Manager, and Account Manager for the City Implementation. Each of these Securus Associates must review the customer provisioning "pre-cut" record, and provide verification and approval.

*An example of the Customer Provisioning Check List can be found in Appendix I.*

#### 5.3.2 Quality Control Checkpoint 2: Customer Pre-Installation

While onsite, the Securus Field Service Technicians will complete a checklist to ensure that the physical installation characteristics meet or exceed Securus standards. Equipment inventory, equipment location, electrical, network/telecom and Video installation standards are reviewed during this checkpoint.

*An example of the Field Tech Check List can be found in Appendix I.*

#### 5.3.3 Quality Control Checkpoint 3: Equipment Testing / Functional Validation

At this stage of the Implementation, the SVV is online and test calls and sessions can be performed. This quality control checkpoint ensures that all SVV calling options are setup to meet the requirements of the City. Test call scenarios are completed and phone labels, call durations, on/off times, administrative terminals, and other customer configurations are verified.

*An example of the Test Validation Check List can be found in Appendix I.*

#### 5.3.4 Quality Control Checkpoint 4: On-Site Customer Acceptance

Our Field Install Team members will perform a walk-through with key City personnel at each location. During this walk-through, the Field Service Specialists will review all the quality control checklists for Quality Control Checkpoints 1-3 and perform a visual inspection of all installed hardware alongside the City personnel.

Any physical installation issues or performance issues will be resolved to the satisfaction of the City personnel.

#### 5.3.5 Quality Control Checkpoint 5: Implementation Acceptance

The final quality control checkpoint involves a review by the City Team. During this review, the Securus Implementation Team will provide copies of all quality control documents, equipment inventory records, network diagrams, issues logs, and final Implementation plan documentation. The Securus Implementation Management Team will host a review of these documents with the City Team. Any outstanding deliverables or service issues will be resolved prior to completing the Customer Acceptance checkpoint.

#### 5.4 Risk Management/Contingencies Plan

*This section of the document provides an overview of the risks will be identified, defined and managed during the implementation project for the City. It defines roles and responsibilities for participants in the risk processes, the risk management activities that will be carried out, the schedule for risk management activities, and the tools and techniques that will be used.*

**5.4.1 Roles and Responsibilities**

<b>Implementation Manager</b>	<p>The Implementation Manager, members of the Implementation Management Team &amp; the City (herein defined as <i>Implementation Team</i>) Team shall meet at the beginning of the Implementation to identify potential risks to the Implementation deliverables and timelines and define mitigation strategies for these risks. The Implementation Team will meet weekly, or as necessary, to review the status of all risk mitigation efforts and review the exposure assessments for any new risk items.</p> <p>The Implementation Manager will be on-site at the start of the project and will attend all schedule meetings with the City staff on-site.</p>
<b>Implementation Member Assigned a Risk</b>	<p>The Implementation Manager will assign each newly identified risk to a Implementation member who will assess the exposure and probability for the risk factor and report the results of that analysis back to the Implementation Manager. Assigned Implementation members are also responsible for performing the steps of the mitigation plan and reporting progress to the Implementation Manager. Reporting activities will be scheduled accordingly - based on the severity of the risk factor.</p>

**5.4.2 Risk Documentation**

<b>Risk List</b>	<p>The risk factors identified and managed for this Implementation will be accumulated in a risk list. The risk list will be produced as part of the Implementation initiation documentation and will be included in the finalized Implementation plan and statement of work.</p>
<b>Risk Data Items</b>	<p>The following information will be stored for each Implementation risk: risk name / ID; description, probability, impact, first indicator that risk is becoming a problem, mitigation approaches, owner, date due, contingency plan.</p>
<b>Closing Risks</b>	<p>A risk item can be considered closed when it meets the following criteria: the planned mitigation actions have been completed and the risk item no longer presents a threat to the defined scope of work.</p>

**5.4.3 Activities**

**Risk Identification**

Task	Participants
<p>The Implementation Team will review the finalized statement of work and define the critical success factors and Implementation milestones. This data will be used to identify potential risks that may prevent the Implementation Team from successfully completing a particular Implementation requirement.</p>	<p>Implementation Team</p>

**Risk Analysis and Prioritization**

Task	Participants
The Implementation Manager will assign each risk factor to an individual Implementation member (based on expertise), who will estimate the probability that the risk could become a problem and the anticipated impact to the Implementation if it does occur.	Assigned Implementation Member
The risk factors are collected, reviewed, and adjusted if necessary.	Implementation Manager
Contingency plans are reviewed and mitigation tactics identified and built into Implementation plan for high-risk scenarios.	Implementation Manager

**Risk Management Planning**

Task	Participants
Those risk factors identified as high risk are assigned to individual Implementation members for development and execution of a risk mitigation plan.	Implementation Manager
For each assigned risk factor, recommend actions that will reduce either the probability of the risk materializing into a problem, or the severity of the exposure if it does. Return the mitigation plan to the Implementation Manager.	Implementation Team
The mitigation plans for assigned risk items are collated into a single list. The completed list is created and made available to all Implementation Members, the City Team, and other interested parties.	Implementation Manager

**Risk Resolution**

Task	Participants
Each individual who is responsible for executing a risk mitigation plan carries out the mitigation activities.	Assigned Individual

**Risk Monitoring**

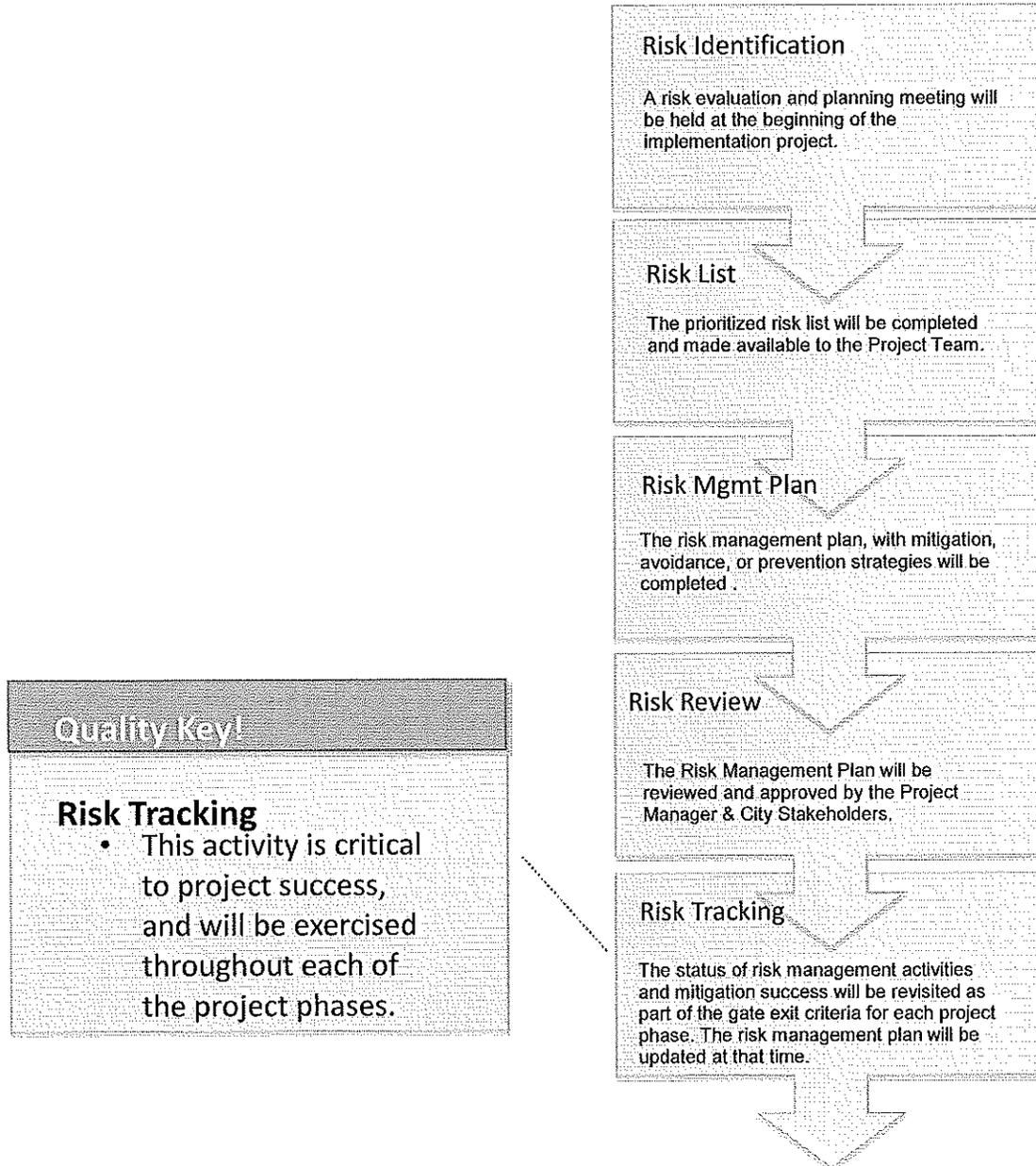
Task	Participants
Key performance indicators will be evaluated within defined intervals in order to gauge risk items.	Implementation Manager
The status and effectiveness of each active mitigation action is reported to the Implementation Manager.	Assigned Individual
The probability and impact for each risk item is reevaluated and modified if appropriate.	Implementation Manager
If any new risk items have been identified, they are analyzed as were the items on the original risk list and added to the risk list.	Implementation Manager
Any risk factors for which mitigation actions are not being effectively carried out, or whose risk exposure is rising, may be escalated to an appropriate level of management for visibility and action.	Implementation Manager / Sales Account Manager / Customer Agent

**Lessons Learned**

Task	Participants
The Implementation Manager will facilitate Lessons Learned discussions following the closure of any risk item which experienced an active mitigation activity.	Implementation Manager

**5.4.4 Schedule for Risk Management Activities**

Note that Dates within the right margin of the activities will be adjusted during the meetings with City. The dates listed show the schedule from another Implementation but give the scope of time frames required.





# Program Management Office Scope of Work

Acceptance

## Acceptance Certificate

Client: City of Denver  
Project:  
Initiated By: Technology Services

Date: \_\_\_\_\_

Milestone Reference:

Type:  Final

Description:

The above \_\_\_\_\_ has been reviewed by the City and fully meets all deliverables and requirements pertaining to its completion as outlined in the entirety of the Statement of Work (SOW) and is hereby considered as having passed the acceptance criteria specified by City.

\_\_\_\_\_  
City Representative Date

\_\_\_\_\_  
City Project Manager Date

\_\_\_\_\_  
Vendor Project Manager Date



CERTIFICATE OF LIABILITY INSURANCE

DATE (MM/DD/YYYY) 11/03/2017

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: Willis of Texas, Inc. CONTACT NAME: ADDRESS: certificates@willis.com INSURER(S) AFFORDING COVERAGE: INSURER A: Zurich American Insurance Company NAIC #: 16535 INSURER B: American Guarantee and Liability Insurance NAIC #: 26247 INSURER C: Lloyd's NAIC #: B7874

COVERAGES CERTIFICATE NUMBER: W4279707 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, EXCLUSIONS AND CONDITIONS OF SUCH POLICIES. LIMITS SHOWN MAY HAVE BEEN REDUCED BY PAID CLAIMS.

Table with columns: INSR LTR, TYPE OF INSURANCE, ADDL SUBR INSD WVD, POLICY NUMBER, POLICY EFF (MM/DD/YYYY), POLICY EXP (MM/DD/YYYY), LIMITS. Rows include Commercial General Liability, Automobile Liability, Umbrella Liability, Workers Compensation and Employers' Liability, and Technology Errors & Omissions.

DESCRIPTION OF OPERATIONS / LOCATIONS / VEHICLES (ACORD 101, Additional Remarks Schedule, may be attached if more space is required) City and County of Denver its elected and appointed officials, employees and volunteers are included as Additional Insureds as respects to General Liability and Auto Liability. General Liability policy shall be Primary and Non-contributory with any other insurance in force for or which may be purchased by Additional Insureds.

CERTIFICATE HOLDER: City and County of Denver, Manager of Safety, 1331 Cherokee Street, Room 302, Denver, CO 80202. 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: [Redacted]

AGENCY CUSTOMER ID: \_\_\_\_\_

LOC #: \_\_\_\_\_



### ADDITIONAL REMARKS SCHEDULE

Page 2 of 2

AGENCY Willis of Texas, Inc.		NAMED INSURED Securus Technologies, Inc. 14651 DALLAS PARKWAY SUITE 600 Dallas, TX 75254	
POLICY NUMBER See Page 1		EFFECTIVE DATE: See Page 1	
CARRIER See Page 1	NAIC CODE See Page 1		

#### ADDITIONAL REMARKS

THIS ADDITIONAL REMARKS FORM IS A SCHEDULE TO ACORD FORM,  
FORM NUMBER: 25 FORM TITLE: Certificate of Liability Insurance

Waiver of Subrogation applies in favor of Additional Insureds with respects to General Liability, Auto Liability and Workers Compensation as per written contract and as permitted by law.



# Notification to Others of Cancellation

Policy No.	Eff. Date of Pol.	Exp. Date of Pol.	Eff. Date of End.	Producer No.	Add'l. Prem	Return Prem.
GLA 1070513-00	09/09/2017	09/09/2018	09/09/2017	36020000	INCL	

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

This endorsement modifies insurance provided under the:

- Commercial General Liability Coverage Part**
- Liquor Liability Coverage Part**
- Products/Completed Operations Liability Coverage Part**

- A. If we cancel this Coverage Part(s) by written notice to the first Named Insured for any reason other than nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation:
  1. To the name and address corresponding to each person or organization shown in the Schedule below; and
  2. At least 10 days prior to the effective date of the cancellation, as advised in our notice to the first Named Insured, or the longer number of days notice if indicated in the Schedule below.
- B. If we cancel this Coverage Part(s) by written notice to the first Named Insured for nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation to the name and address corresponding to each person or organization shown in the Schedule below at least 10 days prior to the effective date of such cancellation.
- C. If notice as described in Paragraphs A. or B. of this endorsement is mailed, proof of mailing will be sufficient proof of such notice.

SCHEDULE	
Name and Address of Other Person(s) / Organization(s):	Number of Days Notice:
BLANKET AS REQUIRED BY WRITTEN CONTRACT	60
OR AGREEMENT	

All other terms and conditions of this policy remain unchanged.

# Notification to Others of Cancellation



Policy No.	Eff. Date of Pol.	Exp. Date of Pol.	Eff. Date of End.	Producer	Add'l Prem.	Return Prem.
GLA 1070513-00	09/09/2017	09/09/2018	09/09/2017	36020000	\$ INCL	\$

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

This endorsement modifies insurance provided under the:

**Commercial Automobile Coverage Part**

- A. If we cancel this Coverage Part by written notice to the first Named Insured for any reason other than nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation:
  - 1. To the name and address corresponding to each person or organization shown in the Schedule below; and
  - 2. At least 10 days prior to the effective date of the cancellation, as advised in our notice to the first Named Insured, or the longer number of days notice if indicated in the Schedule below.
- B. If we cancel this Coverage Part by written notice to the first Named Insured for nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation to the name and address corresponding to each person or organization shown in the Schedule below at least 10 days prior to the effective date of such cancellation.
- C. If notice as described in Paragraphs A. or B. of this endorsement is mailed, proof of mailing will be sufficient proof of such notice.

SCHEDULE	
Name and Address of Other Person(s) / Organization(s):	Number of Days Notice:
BLANKET AS REQUIRED BY WRITTEN CONTRACT OR AGREEMENT	60

All other terms and conditions of this policy remain unchanged.



## Change Endorsement

Policy No.	Eff. Date of Pol.	Exp. Date of Pol.	Eff. Date of End.	Producer	Add'l Prem.	Return Prem.
AUC 1070621-00	09/09/2017	09/09/2018	09/09/2017	36020000	-----	-----

**Named Insured and Mailing Address:**

SECURUS HOLDINGS, INC.  
14651 DALLAS PARKWAY  
DALLAS, TX 75254-8815

**Producer:**

WILLIS OF TEXAS, INC.  
15305 N NORTH DALLAS PARKWAY STE 1100  
ADDISON, TX 75001-6408

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

It is hereby understood and agreed that the following form is added to the policy effective 09/09/2017:

Endorsement # 21 Blanket Notification to Others of Cancellation U-UMB-200-A CW (07/99)

All other terms and conditions remain the same.

# Blanket Notification to Others of Cancellation



Policy No.	Eff. Date of Pol.	Exp. Date of Pol.	Eff. Date of End.	Producer	Addl Prem.	Return Prem.
AUC 1070621-00	09/09/2017	09/09/2018	09/09/2017	36020000	-----	-----

**Named Insured and Mailing Address:**

Securus Hholdings, Inc.  
 14651 DALLAS PARKWAY  
 DALLAS, TX 75254-8815

**Producer:**

WILLIS OF TEXAS, INC.  
 15305 N NORTH DALLAS PARKWAY STE 1100  
 ADDISON, TX 75001-6408

**THIS ENDORSEMENT CHANGES THE POLICY. PLEASE READ IT CAREFULLY.**

- A. If we cancel this policy by written notice to the first **Named Insured** for any reason other than nonpayment of premium, we will deliver electronic notification that such policy has been cancelled to each person or organization shown in a Schedule provided to us by the first **Named Insured**. Such Schedule:
  - 1. Must be initially provided to us within fifteen (15) days:
    - a. After the beginning of the policy period shown in the Declarations; or
    - b. After this endorsement has been added to policy;
  - 2. Must contain the names and e-mail addresses of only the persons or organizations requiring notification that such policy has been cancelled;
  - 3. Must be in an electronic format that is acceptable to us; and
  - 4. Must be accurate.

Such Schedule may be updated and provided to us by the first **Named Insured** during the policy period. Such updated Schedule must comply with Paragraphs 2., 3. and 4. above.
- B. Our delivery of the electronic notification as described in Paragraph A. of this endorsement will be based on the most recent Schedule in our records as of the date the notice of cancellation is mailed or delivered to the first **Named Insured**. Delivery of the notification as described in Paragraph A. of this endorsement will be completed as soon as practicable after the effective date of cancellation to the first **Named Insured** or the longer number of days notice if indicated in the **SCHEDULE** below.
- C. Proof of e-mailing the electronic notification will be sufficient proof that we have complied with Paragraphs A. and B. of this endorsement.
- D. Our delivery of electronic notification described in Paragraphs A. and B. of this endorsement is intended as a courtesy only. Our failure to provide such delivery of electronic notification will not:
  - 1. Extend the policy cancellation date;
  - 2. Negate the cancellation; or
  - 3. Provide any additional insurance that would not have been provided in the absence of this endorsement.

E. We are not responsible for the accuracy, integrity, timeliness and validity of information contained in the Schedule provided to us as described in Paragraphs A. and B. of this endorsement.

<b>SCHEDULE</b>	
<b>Name and Address of Other Person(s) / Organization(s):</b>	<b>Number of Days Notice:</b>
Schedule to be provided by Named Insured as indicated in Paragraph A above.	60

**ALL OTHER TERMS AND CONDITIONS OF THIS POLICY REMAIN UNCHANGED.**

**NOTIFICATION TO OTHERS OF CANCELLATION, NONRENEWAL OR  
REDUCTION OF INSURANCE ENDORSEMENT**

This endorsement is used to add the following to Part Six of the policy.

**PART SIX  
CONDITIONS**

- A. If we cancel or non-renew this policy by written notice to you for any reason other than nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation or non-renewal to the name and address corresponding to each person or organization shown in the Schedule below. Notification to such person or organization will be provided at least 10 days prior to the effective date of the cancellation or non-renewal, as advised in our notice to you, or the longer number of days notice if indicated in the Schedule below.
- B. If we cancel this policy by written notice to you for nonpayment of premium, we will mail or deliver a copy of such written notice of cancellation to the name and address corresponding to each person or organization shown in the Schedule below at least 10 days prior to the effective date of such cancellation.
- C. If coverage afforded by this policy is reduced or restricted, except for any reduction of Limits of Liability due to payment of claims, we will mail or deliver notice of such reduction or restriction to the name and address corresponding to each person or organization shown in the Schedule below. Notification to such person or organization will be provided at least 10 days prior to the effective date of the reduction or restriction, or the longer number of days notice if indicated in the Schedule below.
- D. If notice as described in Paragraphs A., B. or C. of this endorsement is mailed, proof of mailing will be sufficient proof of such notice.

SCHEDULE	
Name and Address of Other Person(s) / Organization(s):	Number of Days Notice:
BLANKET AS REQUIRED BY WRITTEN CONTRACT OR AGREEMENT	60

All other terms and conditions of this policy remain unchanged.

This endorsement changes the policy to which it is attached and is effective on the date issued unless otherwise stated.  
(The information below is required only when this endorsement is issued subsequent to preparation of the policy.)

Endorsement Effective 09-09-17      Policy No. WC 1070512-00      Endorsement No. 001  
 Insured SECURUS HOLDINGS, INC.      Premium \$ INCL.  
 Insurance Company AMERICAN GUARANTEE AND LIABILITY INSURANCE  
 COMPANY

Countersigned By \_\_\_\_\_

entire **Claim** is resolved and the **Insured** obtains a full release on behalf of all the **Insureds** from all claimants.

### III. THE INSURED AND THE INSURED ORGANIZATION

As used throughout this Policy, whether expressed in singular or plural, "**Insured**" shall mean:

- A. The Named Insured listed in Item 1. of the Declarations (the "**Named Insured**") and any **Subsidiaries** of the **Named Insured** (together the "**Insured Organization**");
- B. A director, manager of a limited liability company ("**Manager**") or officer of the **Insured Organization**, but only with respect to the performance of his or her duties as such on behalf of the **Insured Organization**;
- C. An employee (including a part time, temporary, leased or seasonal employee) or **Independent Contractor** of the **Insured Organization**, but only for work done while acting within the scope of his or her employment and related to the conduct of the **Insured Organization's** business;
- D. A principal if the **Named Insured** is a sole proprietorship, or a partner if the **Named Insured** is a partnership, but only with respect to the performance of his or her duties as such on behalf of the **Insured Organization**;
- E. Any person who previously qualified as an **Insured** under III.B., III.C. or III.D. above prior to the termination of the required relationship with the **Insured Organization**, but only with respect to the performance of his or her duties as such on behalf of the **Insured Organization**;
- F. An **Additional Insured**, but only as respects the vicarious liability of such person or entity for the **Insured Organization**;
- G. The estate, heirs, executors, administrators, assigns and legal representatives of any **Insured** in the event of such **Insured's** death, incapacity, insolvency or bankruptcy, but only to the extent that such **Insured** would otherwise be provided coverage under this Insurance; and
- H. The lawful spouse, including any natural person qualifying as a domestic partner under the provisions of any applicable federal, state or local law in the United States, of any **Insured**, but solely by reason of any act, error or omission of an **Insured** other than such spouse or domestic partner.

### IV. TERRITORY

This Insurance applies to **Claims** made and acts, errors or omissions committed, or **Loss** occurring anywhere in the world.

### V. EXCLUSIONS

The coverage under this Insurance does not apply to any **Claim** or **Loss**:

- A. Arising out of or resulting from any criminal, dishonest, fraudulent or malicious act, error or omission, intentional **Security Breach**, intentional violation of a **Privacy Policy** or intentional or knowing violation of the law, if committed by any **Insured**, or by others if such **Insured** colluded or participated in any such conduct or activity;



**DENVER**  
THE MILE HIGH CITY

Office of Human Resources  
Denver's Human Resource Agency

201 W. Colfax, Department 412

Denver, CO 80202

p: 720.913.5751

f: 720.913.5720

[www.denvergov.org/humanresources](http://www.denvergov.org/humanresources)

TO: All Users of the City of Denver Prevailing Wage Schedules  
FROM: [REDACTED], Human Resources Technician II  
DATE: Wednesday, August 30, 2017  
SUBJECT: Latest Change to Prevailing Wage Schedules

Please be advised, prevailing wage rates for some building, heavy, and highway construction trades have not been updated by the United States Department of Labor (DOL) since March 1, 2002. The Career Service Board, in their meeting held on April 21, 2011, approved the use of the attached supplemental wage rates until prevailing wage rates for these classifications of work are again published by the United States Department of Labor.

The attached Prevailing Wage Schedule is effective as of **Friday, August 18, 2017** and applies to the City and County of Denver for **BUILDING CONSTRUCTION PROJECTS** (does not include residential construction consisting of single family homes and apartments up to and including 4 stories) in accordance with the Denver Revised Municipal Code, Section 20-76(c).

General Wage Decision No. CO170030  
Superseded General Decision No. CO20160030  
Modification No. 12  
Publication Date: 8/18/17  
(4 pages)

Unless otherwise specified in this document, apprentices shall be permitted only if they are employed pursuant to, and individually registered in, a bona fide apprenticeship program registered with the U.S. Department of Labor (DOL). The employer and the individual apprentice must be registered in a program, which has received prior approval, by the DOL. Any employer, who employs an apprentice and is found to be in violation of this provision, shall be required to pay said apprentice the full journeyman scale.

For questions call (720) 913-5726.

Attachments as listed above.

General Decision Number: CO170030 08/18/2017 CO30

Superseded General Decision Number: CO20160030

State: Colorado

Construction Type: Building

County: Denver County in Colorado.

BUILDING CONSTRUCTION PROJECTS (does not include single family homes or apartments up to and including 4 stories).

Note: Under Executive Order (EO) 13658, an hourly minimum wage of \$10.20 for calendar year 2017 applies to all contracts subject to the Davis-Bacon Act for which the contract is awarded (and any solicitation was issued) on or after January 1, 2015. If this contract is covered by the EO, the contractor must pay all workers in any classification listed on this wage determination at least \$10.20 (or the applicable wage rate listed on this wage determination, if it is higher) for all hours spent performing on the contract in calendar year 2017. The EO minimum wage rate will be adjusted annually. Additional information on contractor requirements and worker protections under the EO is available at [www.dol.gov/whd/govcontracts](http://www.dol.gov/whd/govcontracts).

Modification Number	Publication Date
0	01/06/2017
1	01/13/2017
2	01/27/2017
3	02/03/2017
4	04/07/2017
5	04/21/2017
6	05/19/2017
7	05/26/2017
8	06/02/2017
9	06/09/2017
10	07/21/2017
11	08/04/2017
12	08/18/2017

ASBE0028-002 07/01/2016

	Rates	Fringes
ASBESTOS WORKER/HEAT & FROST INSULATOR - MECHANICAL (Duct, Pipe & Mechanical System Insulation).....	\$ 29.73	13.93

CARP0055-002 11/01/2016

	Rates	Fringes
CARPENTER (Drywall Hanging		

Only).....\$ 26.25 8.64

-----  
CARP1607-001 06/01/2016

Rates Fringes

MILLWRIGHT.....\$ 31.38 12.70

-----  
ELEC0068-012 06/01/2017

Rates Fringes

ELECTRICIAN (Includes Low  
Voltage Wiring).....\$ 34.70 14.97

-----  
ELEV0025-001 01/01/2017

Rates Fringes

ELEVATOR MECHANIC.....\$ 42.35 31.58

FOOTNOTE:

a. Vacation: 6%/under 5 years based on regular hourly rate for all hours worked. 8%/over 5 years based on regular hourly rate for all hours worked.

b. PAID HOLIDAYS: New Year's Day; Memorial Day; Independence Day; Labor Day; Veterans' Day; Thanksgiving Day; the Friday after Thanksgiving Day; and Christmas Day.

-----  
ENGI0009-017 05/01/2017

Rates Fringes

POWER EQUIPMENT OPERATOR  
(Crane)

141 tons and over.....\$ 29.82 10.10  
50 tons and under.....\$ 27.75 10.10  
51 to 90 tons.....\$ 27.92 10.10  
91 to 140 tons.....\$ 28.55 10.10

-----  
IRON0024-009 05/01/2017

Rates Fringes

IRONWORKER, ORNAMENTAL.....\$ 26.30 12.25

-----  
IRON0024-010 05/01/2017

Rates Fringes

IRONWORKER, STRUCTURAL.....\$ 26.30 12.25

-----  
\* PAIN0079-006 08/01/2017

Rates Fringes

PAINTER (Brush, Roller and Spray; Excludes Drywall Finishing/Taping).....	\$ 20.50	8.41
-----		
* PAIN0079-007 08/01/2017		
	Rates	Fringes
DRYWALL FINISHER/TAPER.....	\$ 21.20	8.41
-----		
PAIN0419-001 07/01/2016		
	Rates	Fringes
SOFT FLOOR LAYER (Vinyl and Carpet).....	\$ 20.00	10.83
-----		
* PAIN0930-002 07/01/2017		
	Rates	Fringes
GLAZIER.....	\$ 31.02	9.37
-----		
PLUM0003-009 06/01/2017		
	Rates	Fringes
PLUMBER (Excludes HVAC Duct, Pipe and Unit Installation).....	\$ 34.53	16.44
-----		
PLUM0208-008 06/01/2017		
	Rates	Fringes
PIPEFITTER (Includes HVAC Pipe and Unit Installation; Excludes HVAC Duct Installation).....	\$ 33.30	17.65
-----		
SFCO0669-002 04/01/2017		
	Rates	Fringes
SPRINKLER FITTER (Fire Sprinklers).....	\$ 36.73	20.47
-----		
SHEE0009-004 07/01/2017		
	Rates	Fringes
SHEET METAL WORKER (Includes HVAC Duct Installation; Excludes HVAC Pipe and Unit Installation).....	\$ 33.26	16.61
-----		
SUCO2013-006 07/31/2015		

	Rates	Fringes
BRICKLAYER.....	\$ 21.96	0.00
CARPENTER (Acoustical Ceiling Installation Only).....	\$ 22.40	4.85
CARPENTER (Metal Stud Installation Only).....	\$ 17.68	0.00
CARPENTER, Excludes Acoustical Ceiling Installation, Drywall Hanging, and Metal Stud Installation.....	\$ 21.09	6.31
CEMENT MASON/CONCRETE FINISHER...	\$ 20.09	7.03
LABORER: Common or General.....	\$ 14.49	5.22
LABORER: Mason Tender - Brick...	\$ 15.99	0.00
LABORER: Mason Tender - Cement/Concrete.....	\$ 16.00	0.00
LABORER: Pipelayer.....	\$ 16.96	3.68
OPERATOR: Backhoe/Excavator/Trackhoe.....	\$ 20.78	5.78
OPERATOR: Bobcat/Skid Steer/Skid Loader.....	\$ 19.10	3.89
OPERATOR: Grader/Blade.....	\$ 21.50	0.00
ROOFER.....	\$ 16.56	0.00
TRUCK DRIVER: Dump Truck.....	\$ 17.34	0.00
WATERPROOFER.....	\$ 12.71	0.00

-----  
WELDERS - Receive rate prescribed for craft performing  
operation to which welding is incidental.

**Office of Human Resources**  
**Supplemental rates**  
**(Specific to the Denver projects)**  
**Supp #101, Date: 11-28-2016**

<b>Classification</b>		<b>Base</b>	<b>Fringe</b>
Boilermakers		\$30.97	\$21.45
Iron Worker, Reinforcing		\$18.49	\$3.87
Journeyman Tile Setter		\$26.83	\$8.48
Laborers: Concrete Saw		\$13.89	-
Paper Hanger		\$20.15	\$6.91
Plasters		\$24.60	\$12.11
Plaster Tenders		\$10.79	-
Power Equipment Operators (Concrete Mixers):			
	Less than 1 yd	\$23.67	\$10.67
	1 yd and over	\$23.82	\$10.68
Power Equipment Operators:			
	Loader up to and incl 6 cu yd	\$23.67	\$10.67
	Motor Grader	\$23.97	\$10.70
	Roller	\$23.67	\$10.67
	Drillers	\$23.97	\$10.70
	Loaders over 6 cu yd	\$23.82	\$10.68
	Oilers	\$22.97	\$10.70
	Mechanic	\$18.48	
Tile Finisher-Floor Grinder- Base Grinder		\$20.87	\$8.42
Truck Drivers	Flatbed	\$19.14	\$10.07
	Semi	\$19.48	\$10.11

- Caulkers—Receive rate prescribed for craft performing operation to which caulking is incidental .i.e. glazier, painter, brick layer, cement mason.
- Use the "Carpenters, Excludes Acoustical Ceiling Installation, Drywall Hanging, and Metal Stud Installation" rates published by the Federal Davis-Bacon rates for batt insulation, pre-stress concrete and tilt up concrete walls.
- Use the "Laborer—Common", for General Housekeeping, Demolition, Final Cleanup and Indoor Fence Installer.
- Trade classification workers cannot be classified as common laborers for performing incidental cleanup from the installation of their craft. Common Laborers perform final cleanup of the entire jobsite.
- Go to [www.denvergov.org/Auditor](http://www.denvergov.org/Auditor) to view the Prevailing Wage Clarification Document for a list of complete classifications used.



**EXHIBIT D**  
**VIDEO VISITATION SCHEDULE**

**This Securus Video Visitation Schedule is made part of and governed by the Video Visitation Services Agreement (the “Agreement”) executed between Securus Technologies, Inc. (“we” or “Provider” or “Securus”) and the City and County of Denver (“you” or “Customer”). The terms and conditions of the Agreement are incorporated herein by reference. This Schedule shall be coterminous with the Agreement.**

**TERMS:**

There is no charge for On-site Visitation. If and when the Customer elects to activate Remote Video Visitation, sessions shall be limited to 30 Minutes, and a session charge of \$8.99, plus applicable taxes/fees/surcharges, will apply to each Remote Video Visitation session; provided, however, that Provider reserves the right, at its sole option, to (i) offer promotional pricing for Remote Video Visitation as low as \$5.00 per session. If Customer wishes to offer free sessions for Remote Video Visitation for any reason other than as allowed pursuant to the Agreement, a session charge of \$8.99 per session, plus applicable taxes/fees/surcharges, will apply and will be invoiced to Customer. As used herein, “Remote” Video Visitation sessions shall mean sessions where the inmate’s visitor is visiting from a location not on the Customer’s premises. “On-site” Video Visitation sessions shall mean sessions where the inmate’s visitor is visiting from a terminal located on Customer’s premises.

When the Customer elects to activate Remote Video Visitation, the Customer will allow Provider to market and promote the use of the Video Visitation System to the inmates, in-person visitors, phone call participants and potential friends and family end users of the System by allowing Provider to (a) distribute Securus’ promotional literature in the Facility’s visitation lobby; (b) unless otherwise prohibited by Customer’s telephone service contract, add a recording to the IVR phone system promoting Securus Video Visitation Services to phone call participants; and (c) issue a joint press release regarding the execution of this Agreement by both parties. All Video Visitation sessions must be scheduled online by the visitor by accessing Provider’s website at [www.securustech.net](http://www.securustech.net).

If applicable, all recorded Video Visitation sessions will have a standard retention of thirty (30) days from the recording date. It is the responsibility of Customer to remove any desired recordings from the housing location for permanent storage within thirty (30) days of their recordings as they may be permanently deleted by Provider after that time. Provider is not responsible for the loss or quality of any such recordings or the deletion of such recordings after thirty (30) days. Further, it is Customer’s sole responsibility to (i) establish and communicate its policies regarding the monitoring and/or recording of private visits (i.e., attorney/client visits, clergy visits or other visits approved and implemented by Customer), and (ii) provide for appropriate accommodations to allow for non-recorded visits, as necessary.

**COMPENSATION:** (Paid Remote Video Visitation Only)

*This Compensation section applies only if Customer elects to activate Remote Visitation.*

Video visitation is not an FCC regulated telecom service; accordingly, in exchange for Customer allowing Provider to utilize Customer’s property and wiring for placement of video visitation terminals, Provider agrees to pay Customer a percentage of the session charges paid to Provider, excluding applicable taxes/fees/surcharges, for Video Visitation sessions placed to Customer’s Facilities as specified in the

chart below (the "Video Visitation Payment). Provider reserves the right to exclude free sessions from the commission calculation. Provider shall remit the Video Visitation Payment for a calendar month to Customer on or before the 30<sup>th</sup> day of the following calendar month in which the paid remote Video Visitation sessions were held (the "Payment Date").

Type of Video Visitation	Video Visitation Payment (Paid Remote Video Visitation Only)
Remote Paid	20%

Customer is responsible for all Jail Management System (JMS) and Commissary integration fees, unless otherwise specified in Attachment 1.

**WARRANTY:** Provider warrants that the Video Visitation services it provides as contemplated in and by this Schedule will be performed in a good and workmanlike manner consistent with industry standards and practices. Provider further warrants that its agent(s) and/or employee(s) utilized by it in the performance of its obligations under this Schedule will be qualified to perform the contracted services. Should any errors or omissions arise in the rendering of the services under this Schedule, Provider will undertake to correct such errors or omissions within a reasonable time period. If Customer purchases from Provider any hardware components in connection with the services hereunder ("Hardware Components"), Provider warrants such components to be free from material defects under normal use, maintenance and service for a period of twelve (12) months from the date of installation of the Hardware Components. This warranty shall be conditional on Customer's compliance with the provisions of this Warranty section.

Provider makes no warranty with respect to low performance, damages or defects in any Hardware Component caused by misuse, misapplication, neglect or accident, nor does Company make any warranty as to any Hardware Component that has been repaired or altered in any way, which, in the sole judgment of Provider affects the performance or purpose for which the Hardware Component was manufactured.

When applicable, Provider shall provide the required replacement parts and components free of charge.

THE WARRANTY OBLIGATIONS OF PROVIDER WITH RESPECT TO THE HARDWARE COMPONENTS ARE STRICTLY LIMITED TO THE REPLACEMENT OF ANY DEFECTIVE HARDWARE COMPONENT. IN NO EVENT AND UNDER NO CIRCUMSTANCES SHALL THE LIABILITY OF PROVIDER FOR HARDWARE FAILURE EXCEED THE UNIT PRICE PAID BY CUSTOMER FOR ANY DEFECTIVE HARDWARE COMPONENT OR PART THEREOF.

EXCEPT AS EXPRESSLY SET FORTH HEREIN OR IN A SCHEDULE TO THE AGREEMENT, THE SERVICES AND ANY HARDWARE COMPONENT TO BE PROVIDED HEREUNDER ARE PROVIDED WITHOUT ANY OTHER WARRANTY OR GUARANTY OF ANY KIND AND PROVIDER DISCLAIMS ANY OTHER EXPRESS OR IMPLIED WARRANTY, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

**OWNERSHIP AND USE.** The Video Visitation System and Software shall at all times remain Provider's sole and exclusive property. Provider (or Provider's licensors, if any) have and will retain all right, title, interest, and ownership in and to (i) the Software and any copies, custom versions, modifications, or updates of the Software, (ii) all related documentation, and (iii) any trade secrets, know-how, methodologies, and processes related to Provider's Applications, the Video Visitation System, and

Provider's other products and services (the "Materials"). The Materials constitute proprietary information and trade secrets of Provider and its licensors, whether or not any portion thereof is or may be the subject of a valid copyright or patent.

**LEGALITY/LIMITED LICENSE AGREEMENT:** For services related to applications which may allow Customer to monitor and record inmate visitation sessions, by providing the application, Provider makes no representation or warranty as to the legality of recording or monitoring such sessions. Customer may utilize settings to disable the monitoring and recording function to prevent monitoring and recording of private sessions (i.e., attorney client privileged communications, clergy visits, etc.) which shall be Customer's sole responsibility to identify, approve and disable. Further, Customer retains custody and ownership of all recordings; however Customer grants Provider a perpetual limited license to compile, store, and access recordings 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, or (iv) maintaining equipment and quality control purposes. This license does not apply to recordings of inmate visitation sessions with their attorneys or to recordings protected from disclosure by other applicable privileges.

### **Schedule 1: ConnectUs Inmate Service Platform**

This Schedule is between Securus Technologies, Inc. ("Provider"), and the City and County of Denver ("Customer" or "you" or "City") and is part of and governed by the Master Services Agreement (the "Agreement") between the parties. The terms and conditions of the Agreement are incorporated herein by reference. **This Schedule shall be coterminous with the Agreement** ("Schedule Effective Date").

#### **CONNECTUS INMATE SERVICE PLATFORM**

##### **DESCRIPTION:**

ConnectUs Inmate Service Platform. ConnectUs is a secure, comprehensive inmate communications and services platform that allows for the consolidation of assorted inmate activities in a single, unified interface with a customized mix of applications ("Applications"). ConnectUs allows inmates to use multiple Applications at the same time and automatically prioritizes scheduled communications events to take precedence over non-scheduled events.

##### **GENERAL TERMS AND CONDITIONS:**

#### **1. PROVISION OF SERVICE**

Provider will make the following Services available to Customer through its ConnectUs Inmate Service Platform (collectively, the "Service") during the Term of the Agreement, subject to the terms of the Agreement, this Schedule and each mutually acceptable written ordering document for the Service executed by both Customer and Provider (each, a "Sales Order Form"): (a) the services ordered by Customer as specified in the Sales Order Form attached hereto as Attachment A and incorporated herein by this reference; and (b) any additional services ordered pursuant to a mutually acceptable amendment to the Agreement executed by both Customer and Provider.

#### **2. GRANT OF RIGHTS; OWNERSHIP OF PROPERTY; USE AND RESTRICTIONS**

**2.1 Grant of Rights.** Subject to the terms of the Agreement and this Schedule: (a) Provider hereby grants Customer a non-exclusive, non-transferable right during the Term of the

Agreement to access and use the Service solely for Customer's internal business purposes as contemplated herein, subject to the Service scope and pricing specified herein and the applicable Sales Order Form; and (b) Customer hereby grants Provider a non-exclusive, non-transferable right to use the electronic data specifically pertaining to Customer and/or its users that is submitted into the Service (collectively, "Customer Data") as necessary for the limited purpose of performing the Service.

2.2 Ownership. Provider and its licensors and suppliers own and retain all right, title, and interest in and to the following (collectively, "Provider Property"): (a) the Service and all other software, hardware, technology, documentation, and information provided by Provider in connection with the Service; (b) all ideas, know-how, and techniques that may be developed, conceived, or invented by Provider during its performance under the Agreement; and (c) all worldwide patent, copyright, trade secret, trademark and other intellectual property rights in and to the property described in clauses (a) and (b) above. Except as otherwise expressly authorized herein or by Provider in writing, the non-exclusive use rights set forth in the Agreement are the entirety of Customer's rights in connection with the Provider Property. Customer owns and retains all right, title, and interest in and to the Customer Data and all intellectual property rights therein. Except as otherwise expressly authorized herein or by Customer in writing, the non-exclusive use rights set forth in the Agreement are the entirety of Provider's rights in connection with the Customer Data.

### 2.3 Use and Restrictions.

- (a) Except as expressly permitted under the Agreement or this Schedule, Customer shall not directly or indirectly do any of the following: (i) access, use, sell, distribute, sublicense, or commercially exploit any Provider Property or any rights under the Agreement, including without limitation any access or use of any Provider Property; (ii) knowingly introduce any infringing, obscene, libelous, or otherwise unlawful data or material into the Service; (iii) copy, modify, or prepare derivative works based on Provider Property; (iv) reverse engineer, decompile, disassemble, or attempt to derive source code from any Provider Property; or (v) remove, obscure, or alter any intellectual property right or confidentiality notices or legends appearing in or on any aspect of any Provider Property.
- (b) At Provider's sole and reasonable discretion, certain of the selected Applications will be made available only during times which would not otherwise interfere with the use of Provider's revenue generating Applications and services.
- (c) Applications ordered by Customer may be disabled by Customer at any time during the Term of the Agreement upon written notice to Provider by an authorized representative of Customer; provided, however, Customer shall remain responsible for paying the Annual Subscription and Hosting Fee according to the Agreement, this Schedule and Sales Order Form(s) set forth in Attachment A, unless otherwise agreed by both parties pursuant to a written and signed amendment.
- (d) Provider may deny the publication of certain documents, videos or forms in connection with the Service, if in Provider's sole and reasonable discretion, such materials are in conflict with the provision of Provider's Service hereunder.
- (e) Customer shall allow Provider to display videos, documents and digital messages to inmates through ConnectUs to promote Provider's new and existing services, products and features.

- (f) Provider is not responsible and hereby disclaims any liability for any and all content of the third party Applications and any documents, videos or forms published by Customer or from outside sources.

### 3. TAX EXEMPTION

- 3.1 Customer agrees to submit a tax exemption certificate to Contractor upon execution of this agreement. If a tax exemption certificate is not provided, Contractor will charge and Customer agrees to pay any applicable sales taxes on all charges to Customer.

### 4. WARRANTIES AND LIMITATIONS

#### 4.1 Service Warranties.

- (a) Provider warrants that the services it provides as contemplated in and by this Schedule will be performed in a good and workmanlike manner consistent with industry standards and practices. Provider further warrants that its agent(s) and/or employee(s) utilized by it in the performance of its obligations under this Schedule will be qualified to perform the contracted services. Should any errors or omissions arise in the rendering of the services under this Schedule, Provider will undertake to correct such errors or omissions within a reasonable time period. If Customer purchases from Provider any hardware components in connection with the services hereunder ("Hardware Components"), Provider warrants such components to be free from material defects under normal use, maintenance and service for a period of twelve (12) months from the date of installation of the Hardware Components.
- (b) Provider makes no warranty with respect to low performance, damages or defects in any Hardware Component caused by misuse, misapplication, neglect or accident, nor does Provider make any warranty as to any Hardware Component that has been repaired or altered in any way, which, in the sole judgment of Provider affects the performance or purpose for which the Hardware Component was manufactured.

#### 4.2 Limitation of Warranty.

- (a) THE WARRANTY OBLIGATIONS OF PROVIDER WITH RESPECT TO THE HARDWARE COMPONENTS ARE STRICTLY LIMITED TO THE REPLACEMENT OF ANY DEFECTIVE HARDWARE COMPONENT. IN NO EVENT AND UNDER NO CIRCUMSTANCES SHALL THE LIABILITY OF PROVIDER FOR HARDWARE FAILURE EXCEED THE UNIT PRICE PAID BY CUSTOMER FOR ANY DEFECTIVE HARDWARE COMPONENT OR PART THEREOF.
- (b) EXCEPT AS EXPRESSLY SET FORTH HEREIN OR IN A SCHEDULE TO THE AGREEMENT, THE SERVICES AND ANY HARDWARE COMPONENT TO BE PROVIDED HEREUNDER ARE PROVIDED WITHOUT ANY OTHER WARRANTY OR GUARANTY OF ANY KIND AND PROVIDER DISCLAIMS ANY OTHER EXPRESS OR IMPLIED WARRANTY, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

- 4.3 Professional Responsibility. As between Customer and Provider, Customer assumes full responsibility for the use of information provided through the Application(s) for patient care. Clinical information, if any, in the Applications is intended as a supplement to, and not a substitute for, the knowledge, expertise, and judgment of professional personnel. Customer acknowledges that the professional duty to the patient in providing healthcare services lies

solely with the healthcare professional providing patient care services. Provider disclaims liability for the use of any information provided by, or results obtained from, the Applications used by professional personnel. Provider, its affiliates and licensors, are not liable for actions of Customer or its authorized users, which may result in any liability due to malpractice or failure to warn. Provider provides no medical or other professional advice in connection with the Applications and the information contained therein. The parties acknowledge that a licensed professional is responsible for independently reaching any medical or other professional judgment and for any resulting diagnosis and treatments, notwithstanding any use of the Applications by such professional.

**ConnectUs Inmate Service Platform**  
**SALES ORDER FORM**  
**SERVICE DESCRIPTIONS**

**APPLICATIONS**

Through ConnectUs, Provider offers the following Applications. (The Applications specifically ordered by Customer are reflected on the Price Page, which follows.)

**Video Visitation Application**

The ConnectUs Video Visitation Application provides video face-to-face visits between inmates and the inmates' friends and family members and also allows the inmate to view upcoming scheduled visits using the ConnectUs touch screen. This Application requires an executed agreement between Provider and Customer for Provider's Securus Video Visitation.

**Inmate Forms (Grievance) Application**

The Inmate Forms (Grievance) Application facilitates the systematic receipt, routing and categorization of grievance situations and offers a tracking system that improves response times and metrics useful in assessments and resource allocations. Provider will retain and provide Customer access to the data for the term of the Agreement.

**Third Party Vendor Commissary Application**

The ConnectUs Third Party Vendor Commissary Application provides an automated means for inmates to order commissary goods through Customer's third-party commissary provider.

**Website Education Application (URL)**

The ConnectUs Website Education Application makes Customer-approved third party educational websites available to inmates.

**Inmate Videos Application (.MP4)**

The ConnectUs Inmate Videos Application enhances communications with inmates by allowing multiple Customer-approved videos.

**Inmate Handbook Application (.PDF)**

The ConnectUs Inmate Handbook Application publishes common PDF documents to inmates (e.g., the Inmate Handbook) for up-to-date access to Customer information.

**Emergency Visitation Application**

The ConnectUs Emergency Visitation Application allows inmates to initiate a request for a video call with Customer staff to report an emergency situation.

**Sick Call Application**

The ConnectUs Sick Call Application allows inmates to report symptoms to Customer health officials by completing a "sick form" that identifies the inmate's symptoms.

**Self-Op Commissary Ordering Application**

The ConnectUs Self-Op Commissary Ordering Application allows Customer to configure its commissary product line within ConnectUs giving inmates an automated means to order commissary goods.

**Job Search Application**

The ConnectUs Job Search Application allows inmate job-seekers access to local, regional and national jobs of all types and level of experience.

**Law Library Application**

The ConnectUs Law Library Application allows inmates to perform legal research through a comprehensive collection of state and federal laws, including resources pertaining to constitutions, statutes, cases and more.

**Securus Inmate Services Platform - Price List**  
**DENVER COUNTY JAIL**

Type	Description	One Time / Recurring	Price/Unit	QTY	Total
Hardware	Video Visitation Terminals - Single Handset (Inmate)	One Time	\$ 4,000	50	\$ 200,000
	Video Visitation Terminals - Single Handset (Visitor)	One Time	\$ 4,000	0	\$ -
	Video Visitation Terminals - Dual Handset (Visitor)	One Time	\$ 4,250	24	\$ 102,000
	Mobile Cart, Including UPS Battery Backup	One Time	\$ 1,440	0	\$ -
Installation and Implementation (Software Application is one time per App, per contract)	Networking Wiring	One Time	\$ 500	74	\$ 37,000
	Electrical Wiring*	One Time	\$ 1,500	0	\$ -
	Hardware Installation	One Time	\$ 500	74	\$ 37,000
	JMS and 3rd Party Vendor Integration**	One Time	\$ -	0	\$ -
	Software Application Setup:	One Time			
	- Securus Video Visitation Application	One Time	\$ 3,975	1	\$ 3,975
	- Phone Call Application	One Time	\$ -	0	\$ -
	- Inmate Forms Application (Grievance)	One Time	\$ 10,000	1	\$ 10,000
	- Inmate Handbook Application (.PDF)	One Time	\$ 3,975	1	\$ 3,975
	- Third Party Vendor Commissary Application	One Time	\$ 3,975	1	\$ 3,975
	- Website Education Application (URL)	One Time	\$ 10,000	0	\$ -
	- Inmate Videos Application (.MP4)	One Time	\$ 3,975	0	\$ -
	- Self-Op Commissary Ordering Application	One Time	\$ 3,975	0	\$ -
	- Emergency Visitation Application	One Time	\$ 3,975	0	\$ -
- Inmate Sick Form	One Time	\$ 3,975	0	\$ -	
Annual Subscription and Hosting Fee (per App, per Terminal, per year)	Securus Video Visitation Application	Recurring	\$ 250	74	\$ 18,500
	Phone Call Application	Recurring	\$ -	0	\$ -
	Inmate Forms Application (Grievance)	Recurring	\$ 500	50	\$ 25,000
	Inmate Handbook Application (.PDF)	Recurring	\$ 250	50	\$ 12,500
	Third Party Vendor Commissary Application	Recurring	\$ 500	50	\$ 25,000
	Website Education Application (URL)	Recurring	\$ 500	0	\$ -
	Inmate Videos Application (.MP4)	Recurring	\$ 250	0	\$ -
	Self-Op Commissary Ordering Application	Recurring	\$ 250	0	\$ -
	Emergency Visitation Application	Recurring	\$ 250	0	\$ -
	Inmate Sick Form	Recurring	\$ 250	0	\$ -
	Job Search Application (annual per App charge)	Recurring	\$ 3,250	0	\$ -
Law Library Application (annual per App charge)	Recurring	\$ 8,000	1	\$ 8,000	
Misc.	Annual Terminal Extended Hardware Maintenance	Recurring	\$ 500	74	\$ 37,000
	Recurring Telecom	Recurring	\$ 5,258	1	\$ 5,258
	Recording Retention (30 days)	One Time	\$ 100	50	\$ 5,000
	On-Site Training (per day)	One Time	\$ 2,000	2	\$ 4,000
				Term:	6
				One-Time Cost	406,925
				Annual License & Maintenance Cost (per year)	131,258
				<b>Total Cost:</b>	<b>\$ 1,194,473</b>
				Securus Investment (discounts; fees waived):	\$ 677,940
				Customer Investment:	\$ 516,533

\* Customer responsible for electrical wiring

\*\* Customer responsible for JMS/Commissary Integration Fees, if applicable

**Securus Inmate Services Platform - Price List  
Downtown Detention Center**

Type	Description	One Time / Recurring	Price/Unit	QTY	Total	
Hardware	Video Visitation Terminals - Single Handset (Inmate)	One Time	\$ 4,000	105	\$ 420,000	
	Video Visitation Terminals - Single Handset (Visitor)	One Time	\$ 4,000	0	\$ -	
	Video Visitation Terminals - Dual Handset (Visitor)	One Time	\$ 4,250	24	\$ 102,000	
	Mobile Cart, Including UPS Battery Backup	One Time	\$ 1,440	0	\$ -	
Installation and Implementation (Software Application is one time per App, per contract)	Networking Wiring	One Time	\$ 500	129	\$ 64,500	
	Electrical Wiring*	One Time	\$ 1,500	0	\$ -	
	Hardware Installation	One Time	\$ 500	129	\$ 64,500	
	JMS and 3rd Party Vendor Integration**	One Time	\$ -	0	\$ -	
	Software Application Setup:	One Time				
	- Securus Video Visitation Application	One Time	\$ 3,975	1	\$ -	
	- Phone Call Application	One Time	\$ -	0	\$ -	
	- Inmate Forms Application (Grievance)	One Time	\$ 10,000	1	\$ -	
	- Inmate Handbook Application (.PDF)	One Time	\$ 3,975	1	\$ -	
	- Third Party Vendor Commissary Application	One Time	\$ 3,975	1	\$ -	
	- Website Education Application (URL)	One Time	\$ 10,000	0	\$ -	
	- Inmate Videos Application (.MP4)	One Time	\$ 3,975	0	\$ -	
	- Self-Op Commissary Ordering Application	One Time	\$ 3,975	0	\$ -	
	- Emergency Visitation Application	One Time	\$ 3,975	0	\$ -	
	- Inmate Sick Form	One Time	\$ 3,975	0	\$ -	
	Annual Subscription and Hosting Fee (per App, per Terminal, per year)	Securus Video Visitation Application	Recurring	\$ 250	129	\$ 32,250
		Phone Call Application	Recurring	\$ -	0	\$ -
Inmate Forms Application (Grievance)		Recurring	\$ 500	105	\$ 52,500	
Inmate Handbook Application (.PDF)		Recurring	\$ 250	105	\$ 26,250	
Third Party Vendor Commissary Application		Recurring	\$ 500	105	\$ 52,500	
Website Education Application (URL)		Recurring	\$ 500	0	\$ -	
Inmate Videos Application (.MP4)		Recurring	\$ 250	0	\$ -	
Self-Op Commissary Ordering Application		Recurring	\$ 250	0	\$ -	
Emergency Visitation Application		Recurring	\$ 250	0	\$ -	
Inmate Sick Form		Recurring	\$ 250	0	\$ -	
Job Search Application (annual per App charge)		Recurring	\$ 3,250	0	\$ -	
Law Library Application (annual per App charge)		Recurring	\$ 8,000	1	\$ 8,000	
Misc.	Annual Terminal Extended Hardware Maintenance	Recurring	\$ 500	129	\$ 64,500	
	Recurring Telecom	Recurring	\$ 9,166	1	\$ 9,166	
	Recording Retention (30 days)	One Time	\$ 100	105	\$ 10,500	
	On-Site Training (per day)	One Time	\$ 2,000	2	\$ -	
				Term:	5	
				One-Time Cost	661,500	
				Annual License & Maintenance Cost (per year)	237,166	
				<b>Total Cost:</b>	<b>\$ 1,847,330</b>	
				Securus Investment (discounts; fees waived):	\$ 951,863	
				Customer Investment:	\$ 895,467	

\* Customer responsible for electrical wiring

\*\* Customer responsible for JMS/Commissary Integration Fees, if applicable

## Enterprise Architecture Technology Standards

### *Our Vision*

*We will become the nation's model for delivery of technology,  
media, and contact center services for local government.*

## Purpose

This Enterprise Architecture Technology Standards document provides the City and County of Denver a framework to mature governance effectiveness and improve service delivery through technical standards.

All listed hardware and software specifications represent the City supported configurations for current and future environments (roughly 6 months).

If the service being proposed does not meet the technical specifications provided in this section, proposals may be submitted; however, a technology exception waiver must be applied for and granted by the Technology Services Leadership Team as a term and condition of the contract. If future compliance is planned (i.e., in a future release of the proposed software or system) please note that clearly in the waiver and in the proposal.

Purpose .....	2
Section I. End User Devices .....	3
1-CCD-01 Desktop, Workstation and Laptop Hardware .....	3
1-CCD-02 Device Software .....	4
1-CCD-03 Mobile Devices .....	4
1-CCD-04 Special Purpose Devices .....	5
Section II. Infrastructure.....	5
2-CCD-01 Communications (Networks, Voice, Video).....	5
2-CCD-02 Compute .....	5
2-CCD-03 Virtualization.....	6
2-CCD-04 Server Operating System.....	6
2-CCD-05 Storage .....	6
Section III. Infrastructure Services.....	7
3-CCD-01 Enterprise Application Control.....	7
3-CCD-02 Domain services (Active Directory, DHCP).....	7
3-CCD-03 Identity management.....	7
3-CCD-04 Data Center .....	7
3-CCD-05 Event Monitoring.....	8
Section IV. Applications .....	8
4-CCD-01 Middleware .....	8
4-CCD-02 Database .....	8
4-CCD-03 GIS.....	8
4-CCD-04 9-1-1 .....	8

## Section I. End User Devices

### 1-CCD-01 Desktop, Workstation and Laptop Hardware

The following specifications are based on the City's existing systems and represent the expected maximum hardware specification for a given class of hardware. These specifications serve as a reference for current and future hardware environment states.

Item	2007 - 2013				2015 - 2018+						
	Basic PC	Advanced PC	WorkStation PC	Standard Laptop	Basic PC	Advanced PC	Workstation PC	Standard Laptop	UltraBook	Workstation Laptop	Tablet
Intel E2140, 1.6GHz	•										
Intel Xeon 5130, 2.0 GHz		•									
Intel Dual-Core Xeon 5160, 3.0 GHz			•								
Intel Core 2 Duo T7100, 1.8 GHz				•							
Intel Quad-Core i5-4590, 3.30 GHz					•						
Intel Quad-Core i7-4790, 3.60 GHz						•					
Intel Xeon Processor E5-2603 v2 Four Core E6-2630, 1.8GHz							•				
4 <sup>th</sup> Gen Intel Core i5-4310U, 2.0GHz, 3M Cache								•			
4 <sup>th</sup> Gen Intel Core i7-4600U, 2.1GHz, 4M Cache									•		
Intel Core i7-4810MQ Processor Quad Core 3.80GHz										•	
Intel Core i3 4020Y Processor 3MB Cache, 1.5 GHz Dual-Core											•
RAM (GB)	2	2	4	2	4	8	16	4	8	8	4
ATI Radeon X300	•										
nVidia Quadro FX 3450, 256 MB		•	•								
Intel X3100 Integrated				•							
AMD Radeon R5 240, 1GB, Half Height, DP & DVI					•						
AMD Radeon R5 240, 1GB, Full Height, DP & DVI						•					
Intel Integrated HD Graphics 4400							•	•	•		
Intel GT2 Graphics											•
AMD FirePro M5100 w/2GB GDDR5										•	
OptiPlex 3040 Desktop Intel® Core™ i5-6500 Processor (Quad Core, 6MB, 4T, 3.2GHz, 65W)											X
Latitude E5570 Intel® Core™ i5-6300HQ (Quad Core, 2.3GHz, 6MB cache)									X		
Surface Pro 4 8GB 256GB i5											X

**1-CCD-02 Device Software**

The City and County of Denver installs and maintains a standard set of software on all desktops and laptops. All software that is acquired by the City and County of Denver must be compatible with the expected environment.

Software Type	Software Name	Technical Requirement
Operating System	Microsoft Windows	Win 7 Professional SP1 64-bit Win 10 Version 1511 and above
Browsers	Internet Explorer	Current Release
	Google Chrome	Current Release
Office Suite	Microsoft Office	O365 Office 2016
Software Framework	Microsoft .NET	Current Release
Java	JRE	Current Release
Adobe	Acrobat Reader	Current Release
	Flash Player	Current Release
	Shockwave	Current Release
Multimedia Framework	HTML 5	Current Release
External Drives	McAfee Encryption	Current Release

**1-CCD-03 Mobile Devices**

The City and County of Denver supports the following mobile devices. Any software that is intended to run on mobile devices should support the following specifications.

Device	Technical Requirement
iPhone	Current Release
iPad	Current Release

Android	Current Release
Windows Phone	Current Release

### 1-CCD-04 Special Purpose Devices

The following specifications represent the expected maximum hardware specification for that class of hardware.

#### Denver Police Department

Hardware Class	Technical Requirement
Processor	Intel Core i5 2.0 GHz 3MB Cache
Memory/Storage	8 GB RAM 256 GB SSD
Display	10.1" WUXGA LED Backlighting Capacitive multi touch w Active Stylus Pen Sunlight Readable 800 Nits
Interface	RFID Reader (UHF 900MHz EPC Gen 2) Magstripe Reader Docking connector
Wireless	Wi-Fi 802.11a/b/g/n/ac Bluetooth v4.0 Integrated 4G LTE with GPS
Durability	MIL-STD-810G/IP65
Warranty	3 Year

## Section II. Infrastructure

### 2-CCD-01-Communications (Networks, Voice, Video)

Available by Consultation

#### 2-CCD-02 Compute

Type	Name	Technical Requirement
Server Hardware	Cisco	UCS
	Oracle	PCA

2-CCD-03 Virtualization

Type	Name	Technical Requirement
Platform	VMWare	ESX 6.0.0
Client	VSphere client	6.0.0
Platform	Oracle VM	Current Release

2-CCD-04 Server Operating System

Type	Name	Technical Requirement
Microsoft	Server	2012 R2
Linux	Red Hat	7 Update
Linux	Oracle	7

2-CCD-05 Storage

Type	Name	Technical Requirement
Backup	CommVault	V10 SP11
File	EMC Isilon	ADC-DAC
Block	EMC Xtreme IO	OneFS

2-CCD-06 End User Device Management

Type	Name	Technical Requirement
Microsoft	System Center Configuration Manager	2012 R2 SP1
IBM	BigFix	9.5

### Section III. Infrastructure Services

#### 3-CCD-01 Enterprise Application Control

Type	Name	Technical Requirement
F5	Big IP	12

#### 3-CCD-02 Domain services (Active Directory, DHCP)

Type	Name	Technical Requirement
Microsoft	DNS	Dynamic DNS Static for Non -Windows Devices
Microsoft	DHCP	IPAM Capable
Microsoft	Active Directory	2008 R2 Schema - Not Forest Functional Level

#### 3-CCD-03 Identity management

Type	Name	Technical Requirement
Microsoft	Active Directory	2008 R2 Schema - <u>Not</u> Forest Functional Level
		Multiple Domain support
	Directory Schema Version	47
Oracle (OIM)	Oracle Identity Manager	11g R2 PS3
	Oracle Access Manager	11g R2 PS3
	Oracle Virtual Directory	11g R2 PS3
	Oracle Internet Directory	11.1.1.4.0

#### 3-CCD-04 Data Center

Type	Name	Technical Requirement
Industry	Telecommunications Labeling	TIA-606-B
Industry	Telecommunications Infrastructure Standard for Data Centers	TIA-942-A

### 3-CCD-05 Event Monitoring

Type	Name	Technical Requirement
Open Source	Op5	Nagios compliant

## Section IV. Applications

### 4-CCD-01 Middleware

Type	Name	Technical Requirement
Microsoft	IIS	8.5
Oracle	WebLogic	12.C
Apache	Tomcat	7.X
Oracle	IDM	12C
Oracle	ODI	12C
Oracle	OBIEE	12C
SAP	Crystal Reports	2013
SAP	BOE	4.2
Oracle	SOA	12C

### 4-CCD-02 Database

Type	Name	Technical Requirement
Microsoft	SQL Server	2014/2016
Oracle	Oracle	12C R2

### 4-CCD-03 GIS

Type	Name	Technical Requirement
ESRI	ArcGIS	10.4.1

### 4-CCD-04 9-1-1

Type	Name	Technical Requirement
Computer Aided Dispatch (CAD)	TriTech Software Systems	V 5.5.22

Voice Recording	Verint	V 5-SP3
Work Force Management (WFM)	Verint	V 15.1

X

[Redacted]

[Redacted]

Director of Enterprise Architecture

X

[Redacted]

[Redacted]

Deputy Chief Information Officer

<b>Vendor Response</b>						
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.				Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Out of the Box	With Configuration	With Custom Programming	Future Release	
		Module				
<b>1 - Scheduling</b>						
1.1	View Schedule/Available Visit Times		X			The Securus Video Visitation platform provides agency users with views on available time-slots based on a selected date by officers/agency users. The scheduling module is conflict-free and does not allow for any double bookings. Additionally, if visitation rules are configured, then a visual warning will appear on-screen.
1.2	Scheduling - Visit Locations, Capacities, etc. a. The specific visit locations in each facility and specify which locations are for inmates and which are for visitors. b. The capacity of each visit area. c. The days of week and times of day visits may be		X			Video Visitation terminals that reside within the inmate housing locations are designated within the platform as "inmate" terminals. Each terminal is assigned to a specific housing location therefore the system can maintain scheduling based on inmate/terminal/location availability. The platform is also capable of maintaining multiple "on-site" visitation locations which allow for a visitor to be physically at the jail and conduct a video visitation session with an inmate at the detention center. The platform takes into consideration the

Vendor Response							
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement. <i>Hover over each column header below for the definition.</i>					
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
		Module					
1.3	Scheduling  The system shall allow DSD System Administrators to set parameters (as defined by DSD) regarding when a social visit can be scheduled for a given date. E.g. A visit can be scheduled no more than 14 days and no less than 7 days in advance of the date requested. Designated DSD personnel shall have the ability to override the parameters on an ad hoc basis, if needed.  The system shall prohibit visits being scheduled for dates that fall outside of the defined range.  The system shall also allow for different parameters to be set for each facility, housing location, etc., as desired.		X				Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.  The Securus Video Visitation platform can be set with parameters such as: not allowing a visit to be scheduled more than 14 days and no less than 7 days in advance. Since the platform utilizes a privilege based structure, designated DSD personnel will have the ability to override said parameters on an ad-hoc basis.  The platform does not allow for different parameters to be set for each housing location - but could be set for each facility (these are site-wide parameters that cannot be configured on a housing location level)
1.4	Scheduling  The system shall have functionality for DSD personnel to easily view which visit times are available and which have already been scheduled, and allow visits to be scheduled only during available times.  If the user chooses to exceed the set scheduling capacity for a specific visit, designated DSD personnel shall have the option to override the limitation on an ad hoc basis		X				The Securus Video Visitation platform has conflict-free scheduling and will not allow for visit time-slots/terminals to be double booked Scheduled start and end times for visitation cannot be modified ad-hoc without submitting a support ticket.

Vendor Response							
Feature	Requirement	Module	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement. Hover over each column header below for the definition.				Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
			Out of the Box	With Configuration	With Custom Programming	Future Release	
1.5	<p>Visit Qualification</p> <p>The system shall allow DSD scheduling personnel to determine if the inmate qualifies for a visit on the date requested based on:</p> <ul style="list-style-type: none"> <li>• Time in the facility (e.g. minimum 10 days)</li> <li>• Housing location</li> <li>• Visit privileges haven't been revoked</li> <li>• Visit quotas E.g. Two visits per weekend (visit limits can vary by housing location)</li> </ul> <p><i>Note: The above listed items. except for visit limits. are</i></p> <p>The system shall allow DSD System Administrators to set a maximum number of visitors allowed per visit (e.g. no more than 3).</p> <p>The system shall automatically prohibit scheduling more visitors than the set limit, however, designated DSD</p>		X				<p>If scheduling is entirely performed by DSD personnel then they can verify their JMS for said parameters and then if approved go ahead and schedule the session. Visit quotas and rules are maintained by the Securus Video Visitation platform.</p>
1.6	<p>Visit Quotas</p> <p>The system shall automatically prohibit scheduling more visitors than the set limit, however, designated DSD</p>		X				<p>Understand and comply - ad-hoc overriding requires DSD permeal to manually schedule the visit rather than public web-based scheduling</p>

Vendor Response							
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
	Module						
1.7	Non-Association Orders					X	SVV does not have an interface for separation orders. Traditionally, sites handle these as they come up
1.8	Real-time schedule updates						The Securus Video Visitation platform will handle schedule modifications/cancellations in a real-time manner and will free-up time-slots as they become available
1.9	Inmate Information						SVV auto-populates the information based on the data sent to Securus from JMS and based on the inmate ID - manual override of information is possible however because of the nature of the interface from the JMS - if each user is defined by visit type upon initially enrolling or scheduling
1.10	Visit Type					X	

		<b>Vendor Response</b>					
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement. <i>Hover over each column header below for the definition.</i>					Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
	Module						
1.11	Visitor Information  When scheduling a visit, the system shall allow the user to enter information for each visitor including, but not limited to: a. Full name (including middle name or middle initial) b. Date of birth c. Government issued ID # (e.g. driver's license, passport, state issued license, military ID, etc.) d. Relation to inmate e. Phone number	X					Fully complies with exception of gov't ID which would a photo rather than entering the actual ID alpha/numerics
1.12	Visitor Information  The system shall be configurable to make certain fields in the visitor information file required fields (e.g. date of birth), where the user must complete the field before the file is created.		X				
1.13	Visitor Master File  The system shall have the capability to set up and retain a single, "master" file for each visitor so that: a. Visitor information can be automatically populated for subsequent visits. b. Notes can be entered for a specific visitor. c. Restrictions can be placed on a specific visitor.  Designated DSD personnel shall also have the ability to edit and update the information in the master file, as	X					Comply with the exception of note entering on specific visitors

**Vendor Response**

For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.

Hover over each column header below for the definition.

Module	Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet
--------	----------------	--------------------	-------------------------	----------------	-------------

Feature	Requirement
1.14 Visitor Master File	The system shall allow the information in the visitor master file to be used for visits with multiple different inmates and across multiple facilities. All visitor files shall be accessible by DSD personnel at both detention facilities.
1.15 Visit Restrictions	The system shall allow visit restrictions to be placed on individual inmates or visitors including: a. A reason for the restriction b. The duration of the restriction
1.16 Visit Restrictions	The system shall allow users to easily view any and all restriction that are in place on either the inmate or a visitor and shall retain a history of all visit restrictions
1.17 Visit Restrictions	The system shall have a way to alert scheduling personnel if an attempt is made to schedule a visit while
1.18 Visit Restrictions	When a new visit restriction is placed on an inmate, the system shall have a way to alert scheduling personnel if the inmate has any visits already scheduled so the visitor(s) can be cancelled or rescheduled

	X				
	X				
	X				
	X				
	X				

Provide a narrative of how meeting each requirement would be achieved. Eg. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.

Permissions based access - accessible at both facilities via any computer with Internet capability and a browser

SVV maintains a robust visitation rule engine. Rules can be imposed site-wide, on housing location, terminal, inmate and visitor levels rules can also be configured with a specific start/end dates

All rules are viewable with appropriate access within the visitation rules page.

a visual warning will appear if an inmate is in a quota restriction or a no-visits allowed situation and will not allow the scheduling to continue with out appropriate The system will alert DSD personnel if a new visitation restriction will affect any upcoming scheduled visits.

		<b>Vendor Response</b>					
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement. <i>Hover over each column header below for the definition.</i>					
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
	Module						
1.19	Inmate Transfers  The system shall have a way to alert DSD scheduling personnel if any inmates that have upcoming visits scheduled are: a. Transferred to a different housing location within the facility b. Transferred to a different DSD facility E.g. from DDC to DCJ c. Transferred to Denver Health Medical Center d. Transferred to a non-DSD detention facility. E.g. State Department of Corrections e. Released	X					Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.  if an inmate is transferred to another housing location the system will receive the new location information from the JMS and will attempt to maintain the same scheduled visit based on availability. if there is not availability (time slot or terminal) - the visit will be automatically cancelled and an email will be sent to the visitor letting them know that it had to be cancelled and will need to be rescheduled.
1.20	Edit Capability  The system shall allow DSD scheduling personnel to make changes to an existing scheduled visit, if needed, including: • Visit date • Visit time	X					The system allows for date and time modifications
1.21	Cancellations  DSD personnel shall be able to cancel scheduled visits and enter a reason (as defined by DSD) for the	X					a prompt will appear asking for a reason for the cancellation - this way it will be logged
1.22	Visit Notes/Comments  The system shall have functionality for DSD personnel to enter notes or comments on a specific visit.					X	No notes can be entered on specific visits

		<b>Vendor Response</b>					
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
		<i>Hover over each column header below for the definition</i>					
Module							
<b>2 - Walk-In Visits</b>							
2.1	Walk-In Visits The system shall allow DSD personnel to enter walk-in visits into the system in accordance with the same policies for scheduled visits (as applicable) such as visit limits, restrictions, etc. The system shall retain a record	X					
<b>3 - Visit Management</b>							
3.1	Printing List of Scheduled Visits The system shall allow DSD personnel to view and print a list of visits scheduled for a given day, time range and	X					the system allows for ad-hoc reporting that can be exported as a PDF, Excel or CSV file which can then be printed
3.2	Visit Duration The system shall allow the designated DSD system administrators to set the default visit duration. E.g. 30 minutes Designated DSD personnel shall have the ability to	X					In order to maintain a conflict-free schedule it is recommended that a constant visitation duration be maintained to allow for the most efficient visitation schedule.
3.3	Visit Kiosk Assignment At visit check-in, the system shall allow DSD personnel to view a grid of the facility's visit kiosks from a control monitor and see which are available to be assigned to the visitor and inmate at the given visit time.	X					At the time of scheduling the Securus Video Visitation platform will schedule and assign a specific terminal for use by the public visitor at a specific time - with the Securus Video Visitation platform there is no need to view which kiosks are available since the system handles
3.4	Visit Kiosk Assignment The system shall allow DSD personnel to change the kiosk assignment at any time before or during a visit.	X					The system allows for kiosk assignment modifications based on availability. (only available kiosks will be shown within the interface to move the visit to)

		<b>Vendor Response</b>					
		For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					
		<i>Hover over each column header below for the definition</i>					
Feature	Requirement	Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
		Module					
3.5	Visit Kiosk Assignment Upon assigning a kiosk to the visitor and the inmate, the system shall have a way to display - on the control monitor and for the duration of the visit - an identifier so the Visit Officer can see <u>who</u> is assigned to each monitor.		X				Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.  The multi session live monitor viewer allows officer with appropriate privileges to view how much time is left on each visit as well as the inmate information and visitor information
3.6	Visit Kiosk Assignment The system shall allow DSD personnel to mark any visit kiosk as "not available" or "not in service" if the kiosk is not to be used for visits for any reason. E.g. if it's not		X				If a terminal repairs Securix will remotely take the unit offline and dispatch a field/onsite tech for repairs
3.7	Delayed Start The system shall allow DSD staff to assign the visit kiosk to the visitor and inmate prior to the visit start time (e.g. when the visitor checks in). The system shall give DSD staff the option to start all visits for a given start time		X				Visit terminals/kiosks, start times, end times (based on set duration) are assigned at the time scheduling.
3.8	Visit Monitoring The system shall allow visits to be visually monitored through the application, in real-time and by displaying a view of both the visitor and inmate simultaneously.		X				The system allows live monitoring of sessions
3.9	Visit Monitoring The system shall allow multiple visits to be visually monitored simultaneously through the application, in		X				The system allows for multiple session live monitoring
3.10	Visit Monitoring The system shall allow the DSD staff monitoring the visit to interrupt the visit with the ability to speak to either the inmate or the visitor - through the application - without the other party able to hear the communication. The application shall also allow DSD personnel to speak to both the visitor and inmate at the same time. The		X				The System has the ability to interrupt the visit. The system does not have the ability to allow DSD personnel speak to the inmate/visitor

		<b>Vendor Response</b>					
		For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					
		<i>Hover over each column header below for the definition</i>					
Feature	Requirement	Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
		Module					
3.11	Visit Monitoring - Mark Visit for Investigative		X				Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.  The system allows for marking of a visit for investigative review
3.12	Pause Visit					X	The Securix Video Visitation platform does not allow pausing of visits in order to maintain a conflict-free and continuous schedule.
3.13	Changing Kiosk Assignment		X				The system allows for modifying kiosk assignment during a visit, without resetting the countdown timer.
3.14	Terminate Individual Visit		X				DSD personnel with appropriate privileges can terminate any visit at any time.
3.15	Terminate All Active Visits					X	
3.16	Adjustable Volume		X				On screen volume controls are available at any time during the video visitation session.
3.17	Visit Countdown Timer		X				Countdown timer is always on at the bottom right hand side of the visitor and inmate screens - no alert is needed since they have a constant countdown letting them know exactly how much time is left for that
3.18	Visit and Visitor Notes		X				

Vendor Response						
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.				
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet
Module						Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
3.19	Visit Status The system shall allow for a status - as defined by DSD - to be placed on a visit and changed/updated as needed such as: - Scheduled - Completed - Canceled	X				Visitation rules and Appointments status report
3.20	Visit Status The system shall have a way to support a visit "close out" process to ensure that the final disposition/status is placed on each visit. (e.g. via alerts, automated reporting, etc.)	X				
<b>4 - Video Recording</b>						
4.1	Automated and Selective Recording The system shall have settings that have functionality to automatically video record all visits but shall also allow designated DSD staff to turn off video recording for a	X				
4.2	Resolution The minimum camera video resolution for each visit monitor shall be 1920 x 1080.	X				High-resolution cameras capable of 1920x1080. For optimal bandwidth utilization recommend 720p @ 30fps.
4.3	ONVIF Compliant Video cameras shall be ONVIF (Open Network Video Interface Forum) compliant, where the cameras are operable with a wide variety of different software	X				
4.4	Digital Recording Video shall be recorded in H.264 format.	X				
4.5	Video-Audio Audio and video shall be synchronized during recording	X				

		<b>Vendor Response</b>					
		For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					
		<i>Hover over each column header below for the definition.</i>					
Feature	Requirement	Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Module					
4.6	Images Per Second Video shall be a minimum of 15 and support up to 30 FPS. Video shall be fluid without any motion blur.		X				
<b>5 - Visit History</b>							
5.1	Visit History The solution shall automatically retain a complete visit history for each inmate and shall include all visits from multiple bookings. The history shall include visits that have been completed, canceled and no-shows. The history shall include all information originally captured when the visit was entered including visit type, date/time, visitor information (e.g. name, relation to inmate), visit disposition (e.g. completed, cancelled) and any notes Visit records from all of an inmate's bookings shall be retained indefinitely even after the inmate has been released or transferred out of either DSD detention Facility.		X				
5.2	Retention						
<b>6 - Reporting</b>							
6.1	Ad-Hoc Reports The system shall allow designated users to generate a variety of reports including ad-hoc reports where report parameters can be defined, via a filter, such as date range, isolate specific data variables, etc., without		X				
6.2	Report Types The system shall support querying visits by a variety of data fields such as by inmate, visitor, facility, housing		X				

Vendor Response							
Feature	Requirement	For each requirement, place an "X" under the category below that best describes how your solution can meet the requirement.					Provide a narrative of how meeting each requirement would be achieved. E.g. What functionality is available out of the box or specifically what configuration or custom programming is needed to meet the requirement, etc.
		Out of the Box	With Configuration	With Custom Programming	Future Release	Cannot Meet	
		Module					
6.3	Multiple Facilities The system shall have functionality to allow users to run a single report that includes visit data from both of the DSD detention facilities. Access to run reports from the system shall be		X				
6.4	Permission Based		X				
6.5	Export Functionality The system shall allow users to export reports into other programs such as Excel, Access, etc.		X				
6.6	Printing Reports The system shall have functionality to allow users to		X				
6.7	Preview Reports The application shall provide the ability to preview reports before printing.		X				
6.8	Save reports The system shall have functionality to save reports to other locations (e.g. local hard drive) and in a variety of formats such as PDF, Word, text, etc.		X				
<b>7 - User Interface and Access</b>							
7.1	User Access DSD staff shall have access to the application via PC from within DSD's facilities and network.		X				
7.2	Inmate/Visitor Interface The solution shall provide an interface for visit participants limited to controlling only basic functions such as adjusting the volume via touch screen, for example.		X				



## ATTACHMENT 3

*DSD Video Visitation Project  
Purpose and Background*

---

# **City and County of Denver**

## **Denver Sheriff Department Video Visitation Project**

### *Background, Objectives and Business Requirements*



## Table of Contents

1.0	Background .....	2
2.0	Project Objectives and Scope .....	2
2.1	Goals and Objectives .....	2
2.2	Project Scope.....	3
2.3	Non-Integrated Solution .....	3
2.4	Visit Kiosk Replacement .....	4
3.0	DSD Visit Policy and Current Process Overview.....	7
3.1	Social Visits.....	7
3.2	Professional Visits.....	8
3.3	Visit Tracking and Record Retention.....	8
3.4	Visit Policy Summary Table.....	9
3.5	Business Users .....	10
4.0	Visit Volumes.....	10

## 1.0 Background

The City and County of Denver (“CCD” or “the City”) Denver Sheriff Department (“DSD”) is looking to replace the video visitation system in two of its detention facilities: Denver County Jail (“DCJ”) and the Van Cise-Simonet Detention Center (“Denver Detention Center” or “DDC”). There are currently two different visitation systems in these facilities, both of which are outdated, unreliable and functionally limited. DSD plans to replace both systems with a single, open-architecture visitation solution, which will be implemented in a phased approach, first at DCJ and then DDC.

The DCJ campus consists of seven buildings with a maximum capacity of 1,450 beds and an average daily occupancy of 700 inmates. DDC consists of one building with a maximum capacity of 1,504 beds and an average daily occupancy of 1,280 inmates.

Roughly 30,000+ social visits and 17,000 professional visits are completed across the two jails annually (estimated). Social visits are conducted via the video systems while professional visits are conducted in person.

CCD does not and is currently not planning to charge fees of any kind for visits.

## 2.0 Project Objectives and Scope

DSD would like to find a single video visitation solution for use in both detention facilities that will support the features and functionality outlined in the corresponding requirements document. Implementation will be completed in a phased approach with initial roll out at DCJ and then DDC.

### 2.1 Goals and Objectives

- Replace unsupported, unreliable and functionally limited systems that are used to manage 30,000+ social visits annually, with a functionally rich solution that supports visit scheduling, visit management, video recording and visit tracking.
- Implement an open architecture solution to allow upgrades and replacement of specific hardware and software components to be completed, as needed, in the future.
- Standardize and streamline the visitation process across both of our detention facilities.
- Maximize visit capacity by replacing unreliable and inoperable equipment.
- Integrate the new solution with DSD’s Jail Management System (JMS) so that inmate information relevant to the visit process can be integrated with the functionality of the new visit system.<sup>1</sup>
- Migrate the complete history of visit records – currently located in the JMS – into the new system so that an inmate’s complete history can be accessed from one place.

- Support DSD and DPD (Denver Police Department) Investigations with enhanced visit data tracking and by expanding the capability to video record visits to both facilities.<sup>2</sup>
- Reduce the movement of inmates by installing visit kiosks inside of the inmate housing pods at DCJ.<sup>3</sup>

1 - DSD plans to replace the existing JMS in 2017, therefore an integration will not be pursued until the new JMS is in place.

2 – Only the visitation system at DDC can currently video record visits as the system at DCJ doesn't have functionality to do so.

3 - The existing kiosks in several buildings at DCJ are located in common areas outside of the housing pods, requiring an officer to escort the inmate to the visit kiosk. (*See Section 2.4*)

## 2.2 Project Scope

### **In Scope:**

- On premise video visitation
- Visit scheduling, visit management, visit monitoring
- Video recording of visits
- Visit tracking (including social and professional visits) and data reporting
- Replacement of electronic components in all visit kiosks in the lobby and inmate housing areas in both facilities (video cameras, monitors, handsets, wiring, etc.) – *See Section 2.4*
- DCJ Only: Replacement of visit stations in the lobby and inmate housing areas (desk, chairs, partitions, etc. – *See Section 2.4*)
- Migration of complete visit history (social and professional visits) from JMS to new visit system

### **Out of Scope:** (*to be completed at a later phase*)

- Online, remote visitation
- Third party or self-service visit scheduling

## 2.3 Non-Integrated Solution

All components of the new solution will be used exclusively to support visit scheduling, management and tracking and will not be integrated with any other inmate service applications (e.g. commissary ordering, inmate phone calling services, etc.)

## 2.4 Visit Kiosk Replacement

### DCJ

DSD plans to replace the existing visit kiosks at DCJ, in their entirety, including the electronic components (cameras, monitors, handsets) and the station itself (chair, desk, partitions). An estimated 24 kiosks will be needed in the facility's lobby and up to 60 in the inmate housing areas.

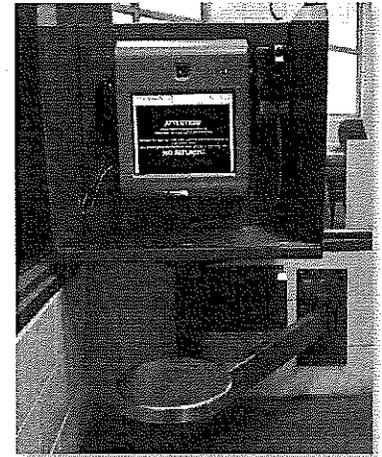
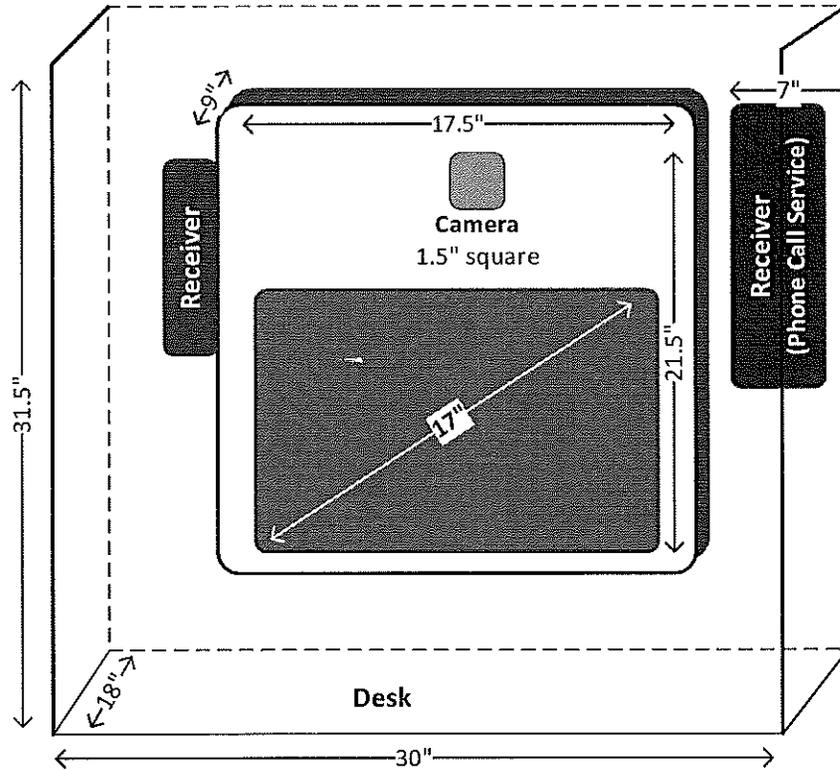
The existing kiosks in several buildings at DCJ are located in common areas outside of the housing pods, requiring an officer to escort the inmate to the visit kiosk. The new kiosks will be installed inside of the housing pods to reduce the movement of inmates.

### DDC

DSD plans to utilize the existing visit stations at DDC (chairs, desks, partitions) and replace only the electronic components (cameras, monitors, handsets, power sources, etc.) for the new visit system. However, each visit station located in the inmate housing areas contains a telephone unit in the upper, right-hand corner of the station. These units provide phone calling services to inmates and are not related in any way to the existing video visitation system. DSD plans to keep these phone units in the kiosks when the new video visitation solution is installed (and will remain separate and non-integrated), therefore, it will be necessary for the electronic components of the new system (monitor, camera, etc.) to be installed in a way that will accommodate these units remaining in the stations.

The new solution will be installed in all 24 visit stations located in the facility lobby and in approximately 93 of the visit stations in the inmate housing areas, all of which are located inside of the housing pods. One of the existing visit stations in each pod will not house the new visit solution but will instead retain the existing hardware and software so inmates have continued access to the commissary and phone call service applications. See **Figure 1** below.

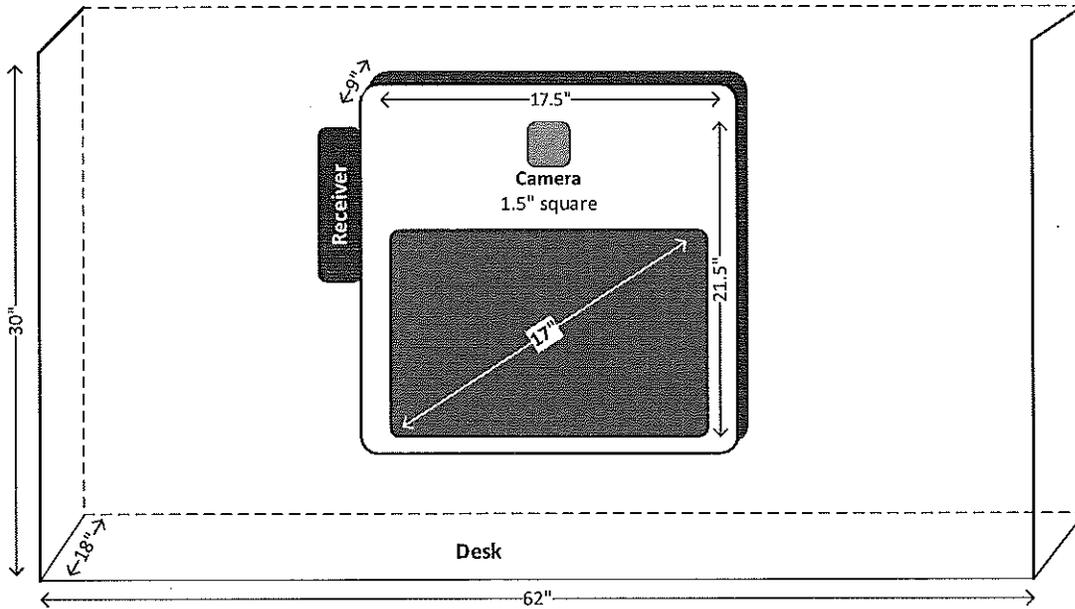
**Figure 1: Visit Station Dimensions – DDC Inmate Housing Areas**



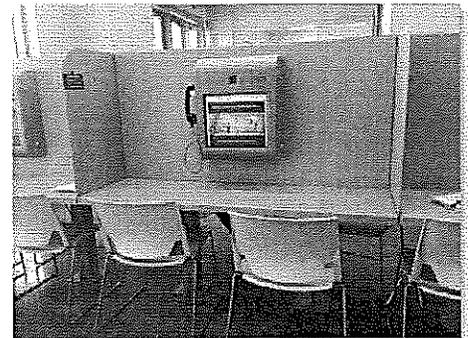
Component	Length	Height	Depth
Desk	30"	n/a	18"
Privacy Partitions	n/a	31.5"	18"
Phone Calling Service Receiver <i>These units will remain in the kiosks but will not be integrated with the video visitation solution.</i>	7" from the right partition to inside edge of phone unit. The unit height is 12".		
Electronics Encasing	17.5"	21.5"	9"
Video Monitor (17")	13.5"	10.5"	n/a
Camera Window	1.5"	1.5"	n/a

The measurements in **Figure 1** are for the visit kiosks located in the DDC inmate housing areas. The dimensions of the encasement that houses the camera and monitor are the same in both inmate and visitor kiosks.

Figure 2: Visit Station Dimensions - DDC Lobby



Component	Length	Height	Depth
Desk	62"	n/a	18"
Privacy Partitions	n/a	30"	18"
Electronics Encasing	17.5"	21.5"	9"
Video Monitor (17")	13.5"	10.5"	n/a
Camera Window	1.5"	1.5"	n/a



Many of the visit stations in the DDC lobby can accommodate two visitors, however, the dimensions of the encasing that houses the electronic components are the same as those in the visit stations located in the inmate housing areas. See **Figure 2** above for specific dimensions.

## 3.0 DSD Visit Policy and Current Process Overview

Both DSD detention facilities permit social and professional visits.

### 3.1 Social Visits

Social visits must be scheduled in advance for both facilities, however, visits are permitted on a walk-in basis at DDC for inmates housed on the 2<sup>nd</sup> floor (excluding Pod 2D). DSD has one full-time Visit Reservationist that manages scheduling for both facilities, which is currently a manual process as the existing visit systems at both jails do not include scheduling modules. The Visit Reservationist manually enters visit information into JMS when the reservation is made.

**Visit Eligibility** – Social visit privileges are based on the following:

- Time in (DCJ only) – The inmate must have been in the facility at least 10 days. If the inmate was transferred from DDC to DCJ, the time at DDC does not count toward the 10 days.
- Housing location – Inmates housed in certain areas of the jail (e.g. special management) may not be eligible for social visits.
- Visit privileges haven't been revoked.
- Visit quotas E.g. Two visits per weekend (visit limits may vary by housing location).

**Video Recorded Visits** - Social visits at DDC are automatically video recorded, saved and available for playback by designated DSD personnel, including Gang Unit Investigators and Internal Affairs. The existing visit system at DCJ does not have functionality to video record visits.

**Visit Quotas** – Inmates are permitted a limited number of social visits in a given week:

- **DCJ:** 2/week, which may consist of 2 single visits or 1 single and 1 group/family visit. The two visits may not be scheduled on the same day. Work Release inmates (Buildings 19 and 24) are permitted 1/week.
- **DDC:**
  - Walk-in visits: 1/day
  - Scheduled social visits: 2/week, which may be either 2 single visits or 1 single and 1 group/family visit. The two visits may not be scheduled on the same day.



### **3.2 Professional Visits**

Professional visits are permitted on a walk-in basis only, 24 hours/day, 7 days/week at both facilities. With the exception of the inmate's attorney, professionals who wish to visit an inmate must obtain permission in advance. The respective jail's Operations team is responsible for processing requests, and permission is typically granted in six-month increments. A separate request is required for each inmate to be visited.

Professional visits are conducted in person and not via the video visitation system.

### **3.3 Visit Tracking and Record Retention**

Inmate visit history, including social and professional visits, is tracked in DSD's JMS since the existing visitation systems at both jails lack functionality to do so. Each visit is manually entered directly into JMS as it is not interfaced with either visitation system.

Visit records are retained indefinitely, even after an inmate has been released, so that a complete visit history is available over multiple bookings.

### 3.4 Visit Policy Summary Table

	Social Visits		Professional Visits
	DCJ	DDC	DCJ & DDC
<b>Reservation Required?</b>	Yes - All visits	Yes - For inmates on floors 3 - 5 and Pod 2D	No - Walk-ins only
<b>Visit Hours Scheduled Visits</b>	<ul style="list-style-type: none"> <li>▪ Fri - Sun Weekly</li> <li>▪ Noon - 8:00 p.m.</li> </ul>	<ul style="list-style-type: none"> <li>▪ Daily</li> <li>▪ 7:00, 8:00, 9:00 a.m. or 6:00, 7:00, 8:00 p.m.</li> </ul>	N/A
<b>Walk-in Visits Permitted?</b>	Not permitted	Permitted for inmates housed on 2 <sup>nd</sup> floor, except Pod 2D	All professional visits conducted on a walk-in basis only.*
<b>Visit Hours Walk-In Visits</b>	N/A	<ul style="list-style-type: none"> <li>▪ Daily</li> <li>▪ 7:00 - 9:00 a.m., Noon - 2:00 p.m. and 6:00 - 8:00 p.m. (first come, first served)</li> </ul>	24 hours/day, 7 days/week
<b>Video or In Person?</b>	Via video system	Via video system	In person
<b>Visit Duration</b>	30 minutes	30 minutes	N/A
<b>Visit Quota</b>	2/week (no more than 1 in a single day), except Buildings 19 and 24 (work release) 1/week	<ul style="list-style-type: none"> <li>▪ Walk-in visits: 1/day</li> <li>▪ Scheduled visits: 2/week (no more than 1 in a single day)</li> </ul>	None

*\* With the exception of the inmate's attorney, professional visitors must obtain approval to visit a specific inmate from the facility's Operations team, which is typically granted for a six-month period.*

### 3.5 Business Users

There will be a total of approximately 50-60 DSD staff members from the following areas that will use the system:

- Scheduling
- DCJ Operations, Classification and Officers
- DDC Operations, Classification and Officers
- DSD Gang Unit Investigations
- DSD Internal Affairs

### 4.0 Visit Volumes

Roughly 30,000+ social visits and 17,000 professional visits are completed across the two jails annually (estimated), with social visits making up about 2/3 of the total volume.

**Figure 3: Visit Volumes**

Annual Visit Totals						
	DCJ		DDC		Both Facilities	
<b>Social Visits:</b>						
Scheduled	6,200	100%	14,300	57%	20,500	65%
Walk-In	-	0%	10,800	43%	10,800	35%
<b>Total</b>	<b>6,200</b>	<b>54%</b>	<b>25,100</b>	<b>68%</b>	<b>31,301</b>	<b>64%</b>
<b>Professional Visits:</b>						
Scheduled	-	0%	-	0%	-	0%
Walk-In	5,300	100%	12,000	100%	17,301	36%
<b>Total</b>	<b>5,300</b>	<b>46%</b>	<b>12,000</b>	<b>32%</b>	<b>17,301</b>	<b>36%</b>
<b>Total Visits</b>	<b>11,500</b>	<b>24%</b>	<b>37,100</b>	<b>76%</b>	<b>48,602</b>	<b>100%</b>