



**SEDGWICK COUNTY  
REQUEST FOR PROPOSAL  
RFP#24-0062 (REVISED)  
INMATE COMMUNICATIONS SERVICES**

DECEMBER 3, 2024 at 1:45 PM CDT

---

**An RFP Solution Prepared for:**

Lee Barrier  
Sedgwick County Purchasing Department  
100 N. Broadway, Suite 610  
Wichita, KS 67202  
purchasing@sedgwick.com

**Presented by:**

Securus Technologies, LLC  
Kevin Elder, President  
5360 Legacy Drive  
Suite 300  
Plano, TX 75024  
972-277-0300

# TABLE OF CONTENTS

<b>COVER LETTER</b>	<b>2</b>
<b>EXECUTIVE SUMMARY</b>	<b>4</b>
<b>I. ABOUT THIS DOCUMENT</b>	<b>6</b>
<b>II. BACKGROUND</b>	<b>7</b>
<b>III. PROJECT OBJECTIVES</b>	<b>8</b>
<b>IV. SUBMITTALS</b>	<b>9</b>
<b>V. SCOPE OF WORK</b>	<b>10</b>
<b>SYSTEM ARCHITECTURE AND DESIGN</b>	<b>113</b>
<b>PROJECT MANAGEMENT</b>	<b>160</b>
<b>TRAINING</b>	<b>170</b>
<b>ARCHITECTURE AND IT STANDARDS</b>	<b>182</b>
<b>PROJECT STATUS REPORTING</b>	<b>198</b>
<b>ACCEPTANCE TESTING</b>	<b>199</b>
<b>DOCUMENTATION</b>	<b>199</b>
<b>USER TRAINING</b>	<b>199</b>
<b>VI. SEDGWICK COUNTY RESPONSIBILITIES</b>	<b>200</b>
<b>VII. PROPOSAL TERMS</b>	<b>201</b>
<b>VIII. REQUIRED RESPONSE CONTENT</b>	<b>211</b>
<b>IX. RESPONSE FORM</b>	<b>223</b>

# COVER LETTER



October 29, 2024  
Sedgwick County Purchasing Department  
Attn: Lee Barrier, Director of Purchasing  
141 W. Elm St  
Wichita, Kansas 67203

## Re: REQUEST FOR PROPOSAL RFP #24-0062 INMATE COMMUNICATIONS SERVICES

Dear Sedgwick County Team:

Sedgwick County Sheriff's Department mission is to maintain a correctional facility with the highest degree of security to ensure the safety of the citizens, your staff, and the inmates in your care. As your incumbent provider, Securus Technologies, LLC (Securus) provided solutions that helped Sheriff Jeff Easter and staff achieve this mission for the last **10** years. We look forward to a continued partnership with Sedgwick County that helps you meet the challenges over the next five years.

Sedgwick County has been instrumental helping develop our core products and services throughout your time as our **valued** partner. We have listened to your concerns and suggestions and developed our newest tablet, the **EVOTAB**. The solution we're proposing meets or exceeds all the specifications set forth by Sedgwick County while offering additional solutions that advance your goals. Sedgwick County and the surrounding community can expect the high-quality communications services you're currently using, with no interruption of service. Our proposal includes several of our advanced investigative tools such as **Word Alert, Digital Mail Center, Inmate Communication Event Report (ICER) and Investigator Pro**, which you are currently using **to assist staff with investigations and prevent future criminal acts.**

- Processed more than 15,000 pieces of mail at our processing center.
- Detected compromised PINs and three-way calling through Investigator PRO
- Detected more than 1,275 inmate-to-inmate calling events through ICER
- Provided 318 suspicious activity reports, which included multiple threats, cell phone contraband, victim tampering, suicidal behavior, and mental health concerns.

Sedgwick County will also have access to features and functions that improve the efficiency of your facility and staff by automating repetitive tasks. We will continue to maintain the existing interfaces that seamlessly integrate with your jail management system and commissary service and will support future interfaces that provide interoperability.

The Sedgwick County Sheriff's Department will realize the following benefits by continuing our partnership:

- **Managed Product Portfolio**—We manage, service, and upgrade our technologies and services using Securus associates, which allows us to respond to requests without waiting on a third party.
- **Increased Staff Efficiency through Technology and Automation**—Securus will continue to deliver web-based applications that enhance and improve efficiency. We will provide ongoing training at no cost so your personnel benefit from all industry-leading technologies, products, and services.
- **Commitment to Evolution**—Providing the newest iteration of our tablet, EVOTAB, to track tablets within the facility, and provide stronger durability and agency control.
- **Unmatched Service and Support**—The most important differentiator in this industry is service. Our commitment to customer service is unmatched. We will continue to support you with our Field Service Technician, Matt Journey, and your full-time onsite Tablet Administrator Damien Ashley. This allows you to focus on what you do best—protect and serve your community.

Over the last 35 years, **we fine-tuned our equipment, technology, support, and service for correctional facilities and law enforcement agencies of all sizes.** We will continue to be agile and progressive to meet the ever-changing needs of industry, including Sedgwick County. Our partners' needs are priority, leading us to provide better technology. Your Senior Account Manager, **Michael Love**, with more than 8 years' experience with Securus, has been responsive to the concerns of Sedgwick County. He can be reached via email at [michael.love@securustechnologies.com](mailto:michael.love@securustechnologies.com) or via phone at (469)-540-0006. Michael, your supporting account team, and I are committed to the success of your mission and goals.

As President of Securus, I am authorized to contractually commit Securus to the terms of this proposal and any resulting contract. Please do not hesitate to contact me with any additional questions, or to request supporting information. You may contact me by telephone at (972) 277-0300, or by email at [kevin.elder@aventiv.com](mailto:kevin.elder@aventiv.com).

**Our innovative technology, services, and solutions will deliver an unmatched experience that brings Sedgwick County value, both today and many years to come.**

Sincerely,

Kevin Elder, President  
Securus Technologies, LLC

# EXECUTIVE SUMMARY

We are pleased to submit our response to the **REQUEST FOR PROPOSAL RFP #24-0062 INMATE COMMUNICATIONS SERVICES** for the Sedgwick County Detention center. Founded in **1986**, Securus has served the inmate communications industry for more than **35** years. More than **3,450** law enforcement, and corrections agencies currently use Securus services and products in all **50** states, including state Departments of Corrections (DOCs).

Securus currently serves **10** agencies within the State of Kansas. Our network of partners allows us to provide extended information sharing capabilities to help support multi-jurisdictional investigations and drive greater shared services among law enforcement departments.

## Services Proposed

Our state-of-the-art end user software, the **NextGen Secure Communications Platform (NextGen SCP)** provides an **anytime/anywhere** accessible solution, which is completely customizable in appearance, function, and individualized security levels set by administrators in an all-in-one, single sign-on application. With numerous features built into the platform, Sedgwick County investigators will easily access call records, debit transaction history, visitation sessions, PINs, and behavior modification tools. With over 700 customizations, Sedgwick County will have every aspect of the communication system at its disposal: **Inmate Telephone System (ITS) – Securus Video Connect (SVC) – EVOTAB Tablet Program.**

## Value Added Services

As you will find outlined in our response, numerous value-added features will be **built into** our proposal. Our proposal has included **Automated Information Services(AIS)** is a hosted interactive voice response (IVR) system which automatically provides correctional information to incarcerated individuals and outside callers over the phone. **Law Library** is also included available on all Video terminals and tablets. Our list of **investigative features such as Word Alert, Investigative PRO(IPRO) and Inmate communications Evaluation report(ICER)**, will be provided to the County at **NO COST**.

Our extensive network of Kansas facilities allow us to provide extended information sharing and **correlation reporting** capabilities, including a cellular chip-off extraction, **(THREADS)** database to help support **multi-jurisdictional investigations. Included** in our proposal you have our industry leading **investigative tools** at your disposal, along with our all new Word Alert **“voice-to-text”** artificial intelligence (AI) assisted and searchable transcription of every call, visitation session and **Securus Text Connect.**

The Sedgwick County investigative team will also have access to the most accurate and continuous **Voice Biometric System** with **Investigator Pro (IPRO)**. IPRO is our powerful voice biometrics software, designed from the ground up with the investigator in mind. Its investigative tools narrow the investigator's search for clues, reducing the time needed to spend listening to calls and pointing them to the calls most likely to help build their case.

Our **Inmate Communication Evaluation & Reporting (ICER)** tool will not only advise you of inmates attempting to connect with each other within your facility, but also from your facility to

another. This is vital to help ensure that **inmates** are not only physically kept apart, but also unable to participate in a three-way communication in attempts to circumvent the rules.

Our **Covert Alert** feature allows staff members with approved security rights to **be notified** upon a target's usage of the system. When the call initiates, it forwards to any number and/or email address with the approved rights to **listen live**.

Securus has also developed a **Background Blur** capability for its Securus Video Connect technology that will legitimately recognize a human face. Securus has succeeded where others have failed, allowing the use of a book cover, magazine photo, or even pencil drawing to access our competitors systems.

As a result, we are confident you will continue that Securus delivers the **most reliable and efficient** inmate communications solutions available, both today and for years to come. Our proposed turnkey solution will meet and **exceed the specifications** set forth by the County. We have tailored our single-source solution to provide robust technologies that will **improve the efficiency** of your facility and ensure the safety and security of staff, inmates, and the public. The solution includes the equipment, connectivity, maintenance, storage, hardware, software, security, training, and all other services needed to ensure the successful installation, implementation, and operation of the County's inmate communications system and services.

As the industry leader in inmate communications, our offer includes a **customizable deployment platform** from phones/visitation terminals on the walls, to phones/visits utilized via our **EVOTAB Tablet**. Our EVOTAB tablet not only allows for calls and video visitation but also educational content/services, self-help and betterment programs, including the ability for K-12 learning management systems, GED/HSE preparation, and College Credit Hours. This includes allowing educators from **local schools** to directly work with incarcerated juveniles and adults to supplement learning. We also introduced **Edovo**. With the capability to assign a device to every single inmate in the Sedgwick County (if desired), the days of sharing communication equipment are over.

## Service and Support

Your **Senior Securus Account Manager**, Michael Love, joined our company in 2016 after a long and successful career in **account management**. Michael is well versed understanding of day-to-day operations, criminal and internal investigations, policy/procedure, training, and most importantly, the expected level of service that must be met by facility vendors, including **24/7/365 availability**. The County will continue to be surrounded with support including your Sr. Account Manager, Client Manager Maronda Parrott, Sr. Director Eddie Valeriano and the entire leadership of our company, to include Chief Executive Officer Dave Abel.

Along with your full-time onsite Securus administrator (and regular visits from other local Field Service Technicians), the Securus Network Operations Center (NOC) will provide **24/7/365 remote monitoring** of all data centers, infrastructure components, platform systems, and inmate phone systems using a suite of network performance monitors. Our Carrollton-based **Technical Support** and **Customer Support** teams are available with **24/7/365** direct line access for your staff and the family members and friends of those incarcerated.

## I. ABOUT THIS DOCUMENT

This document is a Request for Proposal. It differs from a Request for Bid or Quotation in that the county is seeking a solution, as described on the cover page and in the following Background Information section, not a bid or quotation meeting firm specifications for the lowest price. As such, the lowest price proposed will not guarantee an award recommendation. As defined in Charter Resolution No. 68, Competitive Sealed Proposals will be evaluated based upon criteria formulated around the most important features of the product(s) and/or service(s), of which quality, testing, references, service, availability or capability, may be overriding factors, and price may not be determinative in the issuance of a contract or award. The proposal evaluation criteria should be viewed as standards that measure how well a vendor's approach meets the desired requirements and needs of the county. Criteria that will be used and considered in evaluation for award are set forth in this document. The county will thoroughly review all proposals received. The county will also utilize its best judgment when determining whether to schedule a pre-proposal conference, before proposals are accepted, or meetings with vendors, after receipt of all proposals. A Purchase Order/Contract will be awarded to a qualified vendor submitting the best proposal. Sedgwick County reserves the right to select, and subsequently recommend for award, the proposed service(s) and/or product(s) which best meets its required needs, quality levels and budget constraints.

The nature of this work is for a public entity and will require the expenditure of public funds and/or use of public facilities, therefore the successful proposer will understand that portions (potentially all) of their proposal may become public record at any time after receipt of proposals. Proposal responses, purchase orders and final contracts are subject to public disclosure after award. All confidential or proprietary information should be clearly denoted in proposal responses and responders should understand this information will be considered prior to release, however no guarantee is made that information will be withheld from public view.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## II. BACKGROUND

Sedgwick County, located in south-central Kansas, is one of the most populous of Kansas' 105 counties with a population estimated at more than 514,000 persons. It is the sixteenth largest in area, with 1,008 square miles, and reportedly has the second highest per capita wealth among Kansas' counties. Organizationally, the county is a Commission/Manager entity, employs nearly 2,500 persons, and hosts or provides a full range of municipal services, e.g. – public safety, public works, criminal justice, recreation, entertainment, cultural, human/social, and education.

Sedgwick County desires to select a qualified firm who can provide reliable, cost-effective inmate communications which meets or exceeds the requirements described in this RFP. The Sedgwick County Adult Detention Facility is comprised of two (2) physical locations. The Main Facility located at 141 W. Elm St Wichita, KS 67203 and the Annex Facility located at 701 W. Harry St. Wichita, KS 67213. In addition to these two (2) locations, 12 inmate phones will need to be installed and maintained at the Juvenile Detention Center located at 700 S. Hydraulic St. Wichita, KS 67211.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

### III. PROJECT OBJECTIVES

Sedgwick County, Kansas (hereinafter referred to as “county”) is seeking a firm or firms to provide Inmate Communications Services. The following objectives have been identified for this contract:

1. Acquire a turnkey Inmate Communications Service meeting the parameters, conditions and mandatory requirements presented in the document.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus is fully equipped to provide a turnkey Inmate Communications Service that meets all parameters, conditions, and mandatory requirements outlined in this document. We are committed to delivering a comprehensive solution tailored to Sedgwick County’s needs.

2. Establish zero-cost pricing to the county for maintenance, support, installation and professional service hours with the vendor that has the best proven “track-record” in performance, service and customer satisfaction.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus is committed to establishing zero-cost pricing for Sedgwick County regarding maintenance, support, installation, and professional service hours. We have a proven track record of performance, service excellence, and customer satisfaction, guaranteeing that Sedgwick County receives the highest level of support without financial burden.

3. Provide the members of the public a cost-effective means of maintaining contact with friends/family, who are in custody within Sedgwick County.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus is dedicated to providing a cost-effective solution that enables members of the public to maintain contact with friends and family in custody within Sedgwick County. Our services are designed to facilitate meaningful connections while ensuring affordability for all users.

## IV. SUBMITTALS

Carefully review this Request for Proposal. It provides specific technical information necessary to aid participating firms in formulating a thorough response. Should you elect to participate with an electronic response, the RFP number must be entered in the subject line and email the entire document with supplementary materials to:

[purchasing@sedgwick.gov](mailto:purchasing@sedgwick.gov)

Should you elect to participate with a physical response, the response must be sealed and marked on the lower left-hand corner with the firm name and address, bid number, and bid due date. Submit one (1) original AND one (1) electronic copy (.PDF/Word supplied on a flash drive) of the entire document with any supplementary materials to:

Lee Barrier

Sedgwick County Purchasing Department

100 N. Broadway, Suite 610

Wichita, KSD 67202

SUBMITTALS are due NO LATER THAN 1:45 pm CDT, TUESDAY, October 29, 2024. If there is any difficulty submitting a response electronically, please contact the Purchasing Technicians at [purchasing@sedgwick.gov](mailto:purchasing@sedgwick.gov) for assistance. Late or incomplete responses will not be accepted and will not receive consideration for final award. If you choose to send a hard copy of your proposal, Sedgwick County will not accept submissions that arrive late due to the fault of the U.S. Postal Service, United Parcel Service, DHL, FedEx, or any other delivery/courier service.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Proposal responses will be acknowledged and read into record at Bid Opening, which will occur at 2:15 pm CDT on the due date. No information other than the respondent's name will be disclosed at Bid Opening. We will continue to have Bid Openings for the items listed currently. If you would like to listen in as these proposals are read into the record, please dial our Meet Me line @ (316) 660-7271 at 2:15 pm.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## V. SCOPE OF WORK

Items listed in this section are minimum requirements to completion of services under this contract and should not be considered an all-inclusive list. Contractor shall furnish labor, parts

### 1. Inmate Telephones

- a. Shall include without limitation, collect, pre-paid collect, paperless debit interface with commissary provider, international collect calling, and free calling to specific services.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- b. All phones must be ADA compliant, hearing-aid compatible, and have volume control.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our installation engineers will work with Sedgwick County to install our physical equipment that conforms to the accessibility requirements, as directed by Sedgwick County. The traditional phones are shock-resistant, correctional-grade equipment that are hearing aid-compatible, have volume control, and are mounted to ADA standard for wheelchair accessibility, where applicable. In addition, we follow a strict development methodology where the user experience is a cornerstone of all of user interfaces and incorporates the accessibility industry standards where applicable.

- i. All phones and phone accessories must be correctional grade equipment.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus' inmate telephones are designed specifically for the prison environment. The following information is the manufacturer-provided telephone specifications.

### The Industry Standard

The G-Tel model JP-3600 phones are the overwhelming choice for state prison systems, the Federal Bureau of Prisons, county, and city facilities nationwide because of their proven reliability, durability, and flexibility.

### Features/Options

The proposed phone models include the following features:



- Durable 14-gauge stainless steel
- Built-in mounting plate designed for fast, easy installation
- Mounting plate includes gasket which prevents moisture from entering phone
- Oversized line-wire entrance hole w/ moisture-preventing gasket
- Direct wall- or enclosure-mount
- Tamper-resistant locking system
- Oversized, stainless-steel, ADA-compliant keypad
- Adjustable volume button for full ADA compliance
- Magnetic, sealed hookswitch
- Armored handset cord, with internal lanyard, is made to Bellcore standards and withstands minimum 1000-pound pulling test
- Handset cord retaining bracket is designed for fast, easy handset changes
- Stainless-steel grommet provides added security for the handset cord
- Adjustable handset cord lengths, with standard 24" handset length
- Optional noise-canceling microphone available
- Large, customizable instruction card area
- Tested and compliant with FCC Part 15, Subpart B and ANSI C63.4: 2014 standards. FCC Certificate of Conformity number DL-20171166613C

c. All phones will have the ability to capture continuous voice biometric information.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

d. All phones must have the ability to use an integrated PIN assignment and management function that allows all inmate callers to be identified.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

All proposed inmate phones are compatible with PIN usage, allowing callers to be identified.

NextGen SCP authenticates PINs during creation, and again during call validation. Each PIN is linked to an Inmate custody account that contains all information

about the Inmate (e.g., call/video schedules and durations). The PIN is a primary identifier used for behavior modifications, assigning biometric identifiers, and searching communication detail records.

NextGen SCP does not allow duplicate PINs to be created for more than one Inmate custody account. PIN authentication during call validation verifies call/video privileges, identity, facility restrictions on the time allowed between calls to a single number, dialed number/video restrictions, and that the PIN is not already in use. Only after receiving an unrestricted PIN verification from validation will the call/visit proceed. PINs create an audit trail for each communication to show the Inmate who placed the call, the date and time of the call, and the number called.

**i. The Inmate PIN number must interface with JMS to automatically add or change PIN data.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As the incumbent provider of services to Sedgwick County, Securus has already integrated with your existing JMS provider. We will continue to maintain this integration through the next contract term.

**Eliminate manual entry from JMS to NextGen SCP:** Securus NextGen SCP™ automates Inmate personal identification number (PIN) and debit management, through “E-Imports.” The JMS or commissary vendor sends files to an FTP directory at the Securus data center to update the NextGen SCP Inmate profile.

The platform imports Inmate profile information when an Inmate’s status changes, such as at booking, transfer, or release. The facility may also use E-Imports to sell “phone time” through the commissary that automatically transfers to Securus’ Inmate calling debit system.

We support several different types of files, including “booked” files, “released” files, “complete” files, “allowed number” files, and “debit funding” files. The files can be fixed-length or delimited format. E-Imports supports comma-, pipe-, colon-, semi-colon-, and tab-delimited formats.

The facility can send a combination of these files and choose the frequency of file updates. Securus will work with JMS and commissary vendors to determine the specific transfer requirements including file types, file format, and file delivery frequency.

The following is a sample of the information supported by E-Imports:

1. Site ID—facility from which the Inmate is calling. Also used for automatically transferring individuals from one facility to another
2. First name—Inmate's first name
3. Middle name—Inmate's middle name (optional field)
4. Last name—Inmate's last name
5. Birth date—Inmate's date of birth (optional field)
6. Social security number (SSN)—Inmate social security number (optional field)
7. Account number—Inmate's jail ID, booking #, or docket number, to be used as the Inmate custody account number. This is the permanent number provided to the Inmate and does not change if they are released and booked back into the facility.
8. PIN—8- to 16-digit code used to place phone calls. The JMS provides this number to NextGen SCP to allow phone calls.
9. Activate date—date in which the account became active in the system (optional field)
10. Book date—date in which the individual was booked into the facility (optional field)
11. Gender—Inmate gender (optional field)
12. Housing—location of the Inmate (optional field)
13. Race—Inmate race (optional field)
14. Alert level—typically used for security status such as maximum, minimum, low risk, death row (optional field)
15. Max call duration—call duration applied to each phone call placed by this Inmate (optional field)
16. Three-way detection—setting to enable or disable three-way call detection for this Inmate (optional field)
17. Language preference—language in which the Inmate speaks for reporting purposes; does not dictate which prompts are played over the phone (optional field)

- 18. Suspended—setting to allow or prevent the Inmate from placing calls (optional field)
- 19. Suspend start date—start date of calling privileges suspension (optional field)
- 20. Suspend end date—end date of calling privileges suspension (optional field)

Securus recommends sending a combination of all three file formats.

### “Booked” Files

All new custody accounts and changes to NextGen SCP custody accounts trigger the generation of a “booked” file. This file contains only the Inmates added and changed, and should not contain any released Inmates. The following events trigger a “booked” file:

- An Inmate booked into the JMS or transferred to a new site (facility)
- A change to the Inmate account
- Calling eligibility change (Inmate suspended from placing calls)

### “Released” Files

A “released” file sent every time an Inmate is released from the JMS.

### “Complete” Files

A “complete” file contains all active Inmates and their associated information. This file is traditionally sent once a week, to ensure the JMS and NextGen SCP systems are synchronized.

**e. Calls must be recorded and available for review for a minimum of one (1) year.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**f. Call logs and records must be maintained for a minimum of seven (7) years.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Communication records are stored for seven years.

**g. Must include an option for attorneys to request non-recorded calls with clients.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The Securus calling service automatically bypasses monitoring and recording special calls by designating phone numbers, such as those to attorneys, clergy, or doctors, as “private.”

Before installing the calling services product, Securus will seamlessly import all known attorney numbers from your existing system, ensuring no disruption to your operations. Alternatively, if preferred, we can also work with a list provided by the State Bar Association to integrate the attorney numbers into our system. Our goal is to provide a smooth transition while maintaining the integrity of your existing data. The web-based user interface, NextGen SCP™ makes it easy for administrators to maintain this database and, as always, Technical Support is available 24x7x365 to assist with any service needs in maintaining this data. New numbers added are updated for all facilities within the County network.

**Protecting private communications:** NextGen SCP safeguards calls between Inmate and their attorneys. Attorneys can register in a database to classify their phone numbers as private. Depending on whether the attorney completed the registration process, the Inmate and the called party hear one of two warnings:

- Complete registration: *“This is a Private call. It will not be recorded and cannot be monitored.”*
- Incomplete registration: *“This call is not Private. It will be recorded and may be monitored. If you believe this should be a Private call, please hang up and follow facility instructions to register this number as a Private Number. To consent to this recorded call, press ...”*

To further maintain the integrity of attorney-client and other privileged calls, Securus offers an optional patented service called Two-Party Active Consent. Two-Party Active Consent ensures that both the Inmate and called party give their “permission” to record and/or monitor their call.

**h. All rates must be compliant with FCC, state, and local guidelines.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

All proposed rates will comply with FCC, state, and local guidelines.

Securus Technologies is licensed by the Federal Communications Commission as a communications provider and possesses all State and Federal licenses required

of a common carrier of inter-LATA, interstate, and international telecommunications services. Our FCC Federal Registration Number (FRN) is 0006222319.

As an industry leader, we must evolve with the always-changing regulatory climate. To do so, we maintain internal legal and regulatory departments so the products and processes used by our clients are compliant and effective with all emerging trends and regulatory changes that can impact the market. We stay up to date on changes so you can stay up to date with the market.

In July 2024, the Federal Communications Commission issued its final regulations implementing the Martha-Wright Reed Act (the “2024 FCC Order”). The parties acknowledge that the 2024 Order’s requirements impact, among other things, maximum calling rates, the charging of ancillary and other fees, commissions that can be paid to agencies, the types of allowable reimbursement payments that can be made to agencies, and the types of in-kind services providers may not offer to agencies. This RFP response is submitted with pricing that complies with the 2024 FCC Order. The parties agree that, if and when the 2024 Order is overturned or otherwise is no longer in effect in whole or part, the parties will negotiate the terms of this Agreement to the extent possible to address such change, or the agreement will be modified automatically as of the relevant date as necessary and without the need for a written modification of this Agreement to comply with such change.

Please reference Attachment H for more information about our compliance with FCC regulations.

- i. **The reception quality shall meet telecommunication industry standards and shall be at least equal to the quality available to the general public.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus Calling Service through the NextGen SCP™ uses ethernet circuits to provide high-speed connections that transport digitized voice signals, resulting in superior voice quality.

**Greater clarity, better fraud detection/prevention, improved voice verification, and near-perfect sound quality:** Using a mixture of G.711 and G.729a signaling protocol, we dedicate enough bandwidth for each conversation over our dedicated network to keep packet delays under 100 milliseconds. This can achieve a Mean Opinion Score (MOS) of 4.3—better than digitized telephone quality. The quality is transferred directly to our recordings as we use only digital recording equipment for playback of calls; this benefits Sedgwick County in greater clarity, a higher accuracy of fraud detection and prevention, voice verification biometrics, and near-perfect sound quality.

With digital signaling, sound quality is measured as a MOS, which is a subjective measurement derived by averaging ratings given by independent auditors to determine an overall score. Scores range from 1 (poor) to 5 (excellent). The standard for digital telephone quality is considered a score of 3.7 or better. Even though digital signaling allows for better detection of security threats, conversations can still be impaired if there is significant transmission delay. This can happen if signaling uses the public internet or a private system that does not have the necessary bandwidth to support the voice traffic.

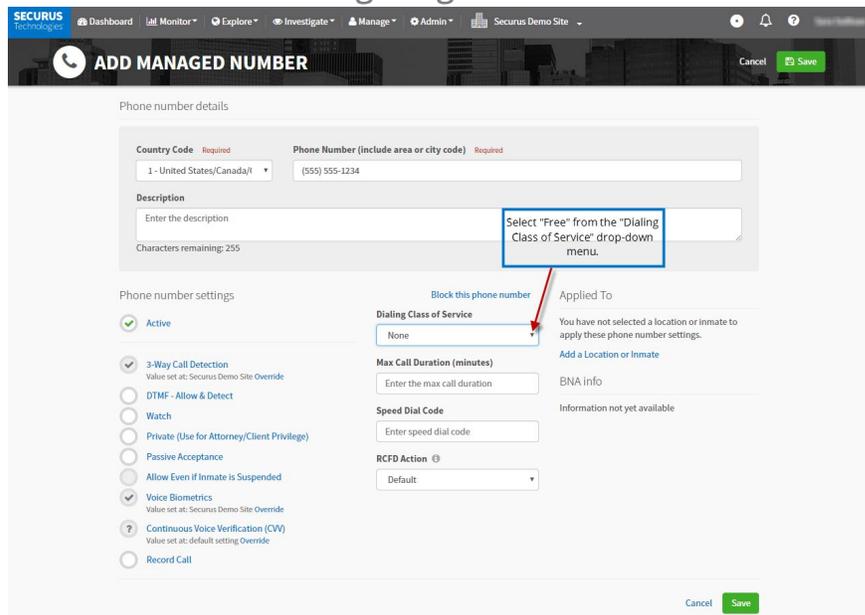
- j. Must have the ability to assign a set number of free calls to each inmate account. A minimum of three (3) free calls will be applied to each account to allow inmates to contact an outside party upon being booked into the jail. These calls will be available to be utilized on all inmate phones.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We will provide free calls to designated individuals, courts, foreign consulates, and other authorized calls, as determined by Sedgwick County. NextGen SCP can provide these calls through any or all inmate telephones so that Sedgwick County staff is not responsible for escorting inmates to a designated telephone. NextGen SCP allows authorized personnel to apply parameters for automated management of the number of calls, call duration, time of day access, and phone(s) used.

Authorized Sedgwick County staff can add numbers to the free call list through the NextGen SCP user interface, as shown in the following figure.

**Configuring Free Calls**



Securus can provide Sedgwick County with the ability to configure free call(s) by both inmate and phone group through the **First Calls Free** feature. This feature was designed to provide an efficient, automated way for staff to:

- Easily comply with legal or regulatory free call requirements
- Manage free calls with no manual intervention
- Prevent the abuse of free calls and the resulting loss of calling revenue

### How It Works

When a new inmate is added to NextGen SCP, or returns after a period of release and the inmate's PIN is re-activated, the inmate will receive their first "X" number of calls free from any phone group where First Calls Free is configured. For example, if Sedgwick County allows each inmate two free phone calls on the group of phones in the booking area, NextGen SCP will allow those two calls at no charge. The third phone call would incur charges, as would any calls made outside the booking area.

Other advantages of First Calls Free are:

- NextGen SCP only recognizes the free call if the call is connected to the called party, ensuring the inmate can instruct the called party on how to set up a prepaid AdvanceConnect® account
- It is configurable by both number of free calls and phone groups, providing facilities with complete free call control
- Free calls are subject to all number blocking, and inmate suspension restrictions

## Configure First Calls Free in NextGen SCP

The screenshot shows the 'ADD NEW INMATE' form in the NextGen SCP interface. The form is divided into several sections: Inmate Status (Active), Inmate Details (Site, Housing Unit, Inmate Account Number, Inmate First Name, Inmate Middle Name, Inmate Last Name, Date of Birth, Social Security Number), and Call Management. The Call Management section includes options for 'First Call Free? (1 allowed)', '3-way Calling Detection', and 'Private (on visitation)'. The 'First Call Free? (1 allowed)' option is selected, and a blue box highlights the text 'Select "First Calls Free" when creating a new inmate account.' with a red arrow pointing to the selected radio button. Other options include 'Maximum Call Duration (minutes)' set to 12, 'Recorded Name Information', 'Investigator Pro CW', and 'RCFD Action' set to Default.

## Calling Restrictions

Every call type is subject to defined calling restrictions, including free calls. Sedgwick County can also limit how many free calls an inmate can make in a specified period. Other restrictions that can be applied to free calls include:

- Limiting the number of free calls that can be connected, regardless of called party acceptance status
- Limiting the number of free calls the called party positively accepts

NextGen SCP will also allow Sedgwick County to define how often the calling restrictions reset. The number of free call connects or accepts can be configured to reset:

- Daily
- The "daily" reset can be configured by the number of days. For example, every three days an inmate can place one accepted free call
- Weekly
- Monthly

Authorized Sedgwick County users can specify what day of the month or week the rule is reset.

## Configuring Free Call Restrictions in NextGen SCP

**CREATE CALL RESTRICTION**

Call Restriction Name Required  
Free Calls for John Doe

Status  
 Active

Add Rule

Description Required

Restriction Resets Required  
Daily **every**  day(s)

Allowed Call Types Required  
Free Calls

Limits (you must set at least one of the following)  
 Call Accepts  
 Successful Connections  
 Talk Time (minutes)

### Free by Dialed Phone Number

Any phone number can also be set as free from the “Managed Number” page. Clicking “Add a Location or inmate” opens a window to choose the location—facility, site, terminal group—or inmate to which free calls will apply, as shown in the following image.

### Setting Free Calls in Global Lists

**MANAGE PHONE NUMBER LOCATION OR INMATE**

Select one or more facilities, sites, and/or inmates to apply this managed phone number. This action will replace any existing phone number setting for the selected location(s).

Locations

- Facilities **Select "Facilities" from the "Locations" menu**
- Sites
- Terminal Groups
- Inmates

Select Facilities

**Securus Demo Site** **Select the desired facility.**

Selected

Facility: 1  
Securus Demo Site

**Click "Save."**

## Free Phones and Free Local Phones

Securus staff can also configure any phone group as a “Free” phone group or “Free Local” phone group. After creating a group, Securus can add any phone to it. Inmates can place local, intraLATA, interLATA, or interstate calls from the “Free” phone group at no cost to the inmate or called party. Calls made by inmates in a “Free Local” phone group to called parties outside the local area would incur charges.

- k. **All phone calls will contain a recorded message informing both the outside party and the inmate that all calls are recorded and subject to monitoring.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

When a called party answers, the Securus calling service announces that they are receiving a collect call from an inmate, along with the name of the institution. As the incumbent provider, Securus utilizes the inmate’s pre-recorded name, already stored in our system, which is played to the called party as part of the call acceptance message to ensure clear identification of the calling inmate.

For example, a typical announcement would say, *“You have a collect call from an inmate, “John Doe,” at the Sedgwick County. This call is not Private. It will be recorded and may be monitored. If you believe this should be a Private call, please hang up and follow facility instructions to register this number as a Private Number. To consent to this recorded call, press...”*

Call prompts are played twice and each facility can customize the facility name used in call announcements.

- l. **All audio prompts on the phone must be available in at least English and Spanish.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The Securus calling service default system setup provides message prompts in both English and Spanish. Inmates select a specific language at the beginning of the call process by dialing a single digit. Securus offers 15 different language choices to meet their specific need.

During call acceptance, the called party receives the acceptance instructions first in English and then receives an option to continue in the language the Inmate selects. This fraud deterrent feature eliminates possible attempts by the Inmate to confuse the called party with a language they do not understand.

Securus provides durable printed dialing instructions in both English and Spanish on each Inmate telephone, using appropriate materials and techniques for the correctional environment that clearly explains the process in a manner that is easy to read and understand:

### Sample Dialing Instructions in English and Spanish

This Call is Being Recorded	Esta Llamada será grabada
<p><b>DIALING INSTRUCTIONS</b></p> <p>Press "1" for English</p> <p>For a collect call, press "1"</p> <p>For a debit call, press "2"</p> <p>TIPS Hotline, press "8"</p> <p>Enter your PIN</p> <p>Enter your area code and phone number</p> <p>You may hear silence during the acceptance of your call. Please continue to hold.</p>	<p><b>INSTRUCCIONES DE MARCADO</b></p> <p>Presione "2" para español</p> <p>Para llamada por cobrar, presione "1"</p> <p>Para llamada de débito, presione "2"</p> <p>Para línea directa de aviso secreto, presione "8"</p> <p>Introduzca su número de identificación personal</p> <p>Introduzca su número de teléfono, incluyendo el código de área</p> <p>Escuchará silencio mientras su llamada es aceptada. Continúe esperando por favor.</p>

m. A minimum of three (3) portable phones will be provided for use throughout the facility. The portable phones must be attached to cart allowing it to be transported throughout the facility.

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We will provide a roll-away phone mounted to a roll-around pedestal, in a four-wheel design or a two-wheel design, as shown.

The phone can also be mounted to a hand truck (dolly).



## 2. Video Visitation Machines

- a. All video visitation equipment must be wall mounted.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

### EVOTAB Terminal



Concept Only, Design and Product Not Final

#### Software features include:

- Current and future EVOTAB apps and functions are supported, including VRS, SVC, outbound Videograms, and mirrors the same, familiar log-in process as the EVOTAB Tablet.
- Portrait mode is available for all applications while remaining ADA compliant.
- Customizable permissions allow facilities to limit specific applications or disable the entire terminal.
- Manage scheduled video visitations with the Conflict Management feature to facilitate transitioning inmates off a terminal before a scheduled video visitation is to start. Controls are configurable based on facility preference.

**Providing easy-to-access and easy-to-maintain technology solutions:** With our solutions, onsite Securus administrators can replace terminals while maintaining security standards. Plus, with 24x7x365 secure monitoring supported by Securus staff, our solutions are safe, reliable, and protected.

On top of easy administration, the wall-mounted tablet solution also provides your incarcerated users with a familiar experience that mirrors their Personal tablet interface. Here's a look at the incarcerated user's experience:

- A video connect session is scheduled by family and friends through Securus Online or the Securus Mobile App
- The system automatically assigns the video connect session to a wall-mounted tablet.
- The incarcerated user will receive a notification alerting them that they have an upcoming video connect session scheduled. The notification will include information on which wall-mounted tablet their session has been assigned to.
- When it's time for the scheduled video connect session, the incarcerated user simply logs into the assigned wall-mounted tablet and participates in the video session.
- Once the video connect session is complete and the call is terminated, the wall-mounted tablet automatically locks and signs the incarcerated user out.
- The wall-mounted tablet returns to available status and is ready for the next scheduled video connect session.
- Securus' Video Connect platform will undergo a major update in 2025. Please talk with your Account Manager for more details about this plan.

**b. All video visitation equipment must be correctional grade with no removable exterior parts.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our video visitation equipment is all correctional grade with no removable parts. Please reference response to 2(a) for more information about Securus video visitation equipment.

**c. Must be able to interface with commissary and inmate banking providers.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As the incumbent provider at Sedgwick County, we already integrate seamlessly with commissary and inmate banking providers. Our solution ensures secure, real-time transactions and accurate fund management. With established integrations, we guarantee a smooth transition and continued efficient operations at the facility.

**d. Must have the ability for facial recognition and to blur out background around visiting individuals.**

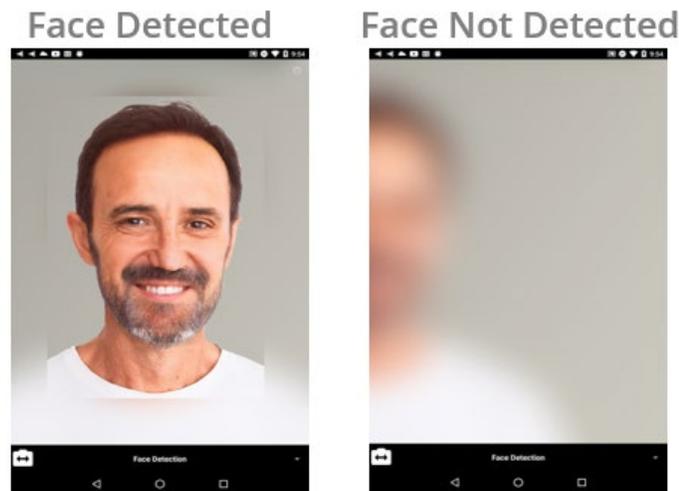
**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Maintain safety and security at Sedgwick County facilities:** Face in Frame detects faces in the camera view for the inmate and the video guest.

How it works:

1. When the camera detects a face in its field of vision, the face is clear and visible while the background and area around the face will be blurred.
2. When a face is not detected within the camera’s field of vision, the entire screen is blurred. When this happens, audio is still supported—users can hear each other but cannot see each other clearly.

With facial detection technology, Face in Frame **blurs any potential nefarious activity** that may be happening in a user’s background during video sessions. This added layer of security is another way we’re optimizing our products to support Sedgwick County’s goals of **maintaining safety and security** at your facilities.



- e. Must provide a minimum of 12 visitation kiosks in the main jail lobby to facilitate free video visits with members of the public.

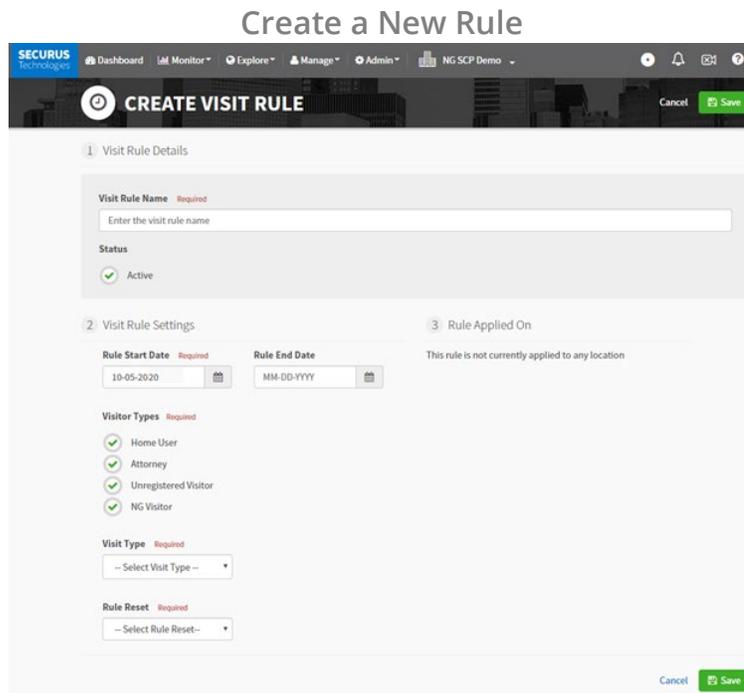
**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus will continue to provide a minimum of 12 visitation kiosks in the mail jail lobby to facilitate free video visits with members of the public.

- i. Each inmate will be allowed one (1) hour of free on-site video visitation with members of the public. The one (1) hour will be divided into three (3) 20 minute visits.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Sedgwick County can allow each inmate one free hour of onsite video visitation with members of the public, as required. While in the Visit Rules section, click on “Create Visit Rule” to create a new Rule.



From here, you will define a rule name, and configure the following fields:

- **Status:** Active or inactive
- **Visit Rule Settings:** select the date for the rule to start and stop.
- **Visitor Types:** Home user, attorney, unregistered visitor, visitor
- **Visit Type:**

- Onsite: Standard on-site visit
- Remote: Applies to both friends & family home user and attorney home user
- **Rule Reset:** Daily, weekly, or monthly
- **Rule Applied On:** Apply the rule to a specific location

Users create a new rule without an initial association. The rule will not be in effect until there is, at least, one entity associated. Associations, in order of priority, are as follows:

- **Inmate Association:** Rule applies to a specific Inmate or user
- **Visitor Association:** Rule applies to specific visitor
- **Terminal Association:** Rule applies to a specific terminal. \*
- **Terminal Group Association:** Rule applies to a specific location such as a pod. \*
- **Visitor Type Association:** Rule applies to every member of the user group to which the rule is associated
- **Site Association:** Rule applies to a specific Site. \*
- **Facility Association:** Rule applies to the entire facility.

*\*The behavior of rules is cumulative.*

Rules are prioritized based on the association level in which they are applied. For example, a visit rule applied to an Inmate (highest priority) takes higher priority than a rule associated with a site. This means that if there is a site-level rule that allows Inmates to have one onsite visit per month and an Inmate-level rule for a specific Inmate to have five onsite visits per month, the user level rule would take priority.

Example Visit Rule:

- Rule Name: 2 Visits per Week
- Visit Type: Onsite
- Quantity: 2
- Frequency: 1
- Duration: Week

Reads: 2 onsite visits per 1 week

If two rules with the same priority conflict, both rules will need to pass to schedule an appointment. An example of this conflict is an Inmate visit rule to allow one onsite visit per week and an Attorney Visitor Type visit rule that allows five onsite visits per week. Both rules must pass to schedule a visit.

### Associating Visit Rules

Enforcement of a Visit Rule requires association with a facility, site, terminal group, terminal, Inmate, visitor, or visitor type. Associations are easily applied while managing each of those.

### Editing Visit Rules

Editing or deleting a visit rule can be accomplished through the Admin > Visit Rules menu.

When editing a visit rule, you can modify all components of the rule. A popup showing the number of impacted sessions, if any, appears before saving a rule change. This prevents the unintentional cancellation of previously scheduled visits.

### Logging

The NextGen SCP logs all changes to Visit Rules, and this log is accessible from the Explore > System Logs menu.



Example log outputs include:

### Example Log Output

The screenshot displays the SECURUS SYSTEM LOGS SEARCH interface. The search criteria are set to "Log Date Range (PT) Required" from 01-01-2020 12:00 AM to 04-29-2020 11:59 PM. The results table shows two entries:

Product	Log Type	Log Type Description	By User	Date/Time (PT)
SW	Data Changes	Visit Rule Created	[Redacted]	04-21-2020 11:22:48 AM
SW	Data Changes	Visit Rule Created	[Redacted]	03-25-2020 8:18:00 AM

The details panel on the right shows the following information:

- User: [Redacted]
- Username: [Redacted]
- Log Date/Time: 03-25-2020 8:18:00 am PDT
- IP Address: [Redacted]
- Action: Visit Rule Created
- Type: Add
- 2 On-Site visits per week
- Alter:
  - Rule Name: 2 On-Site visits per week
  - Active: True
  - Start Date: 03-25-2020
  - End Date: 03-25-2025
  - Visitor Types: Home User, Unregistered Visitor
  - Visit Type: Onsite (2)
  - Reset Duration: Monday
  - Reset Frequency: Week

## Bypass Visitation Rules and Buffer

NextGen SCP allows authorized facility administrative users to bypass visit rules and visit buffers when scheduling appointments.

### Bypass Visitation Rules

The screenshot shows the SECURUS CREATE VISIT interface. The process flow includes: Inmate, Visit Type Onsite, Visitor, Visitor Details, Date & Time, and Confirm. The "Visitor Terminal Group" is set to "MRK Visitor Center". Under "Visit Options", the "Duration" is set to "Required". The "Overrides" dropdown menu is open, showing the following options:

- None Selected
- All
- Bypass Visitation Rules
- Bypass Visitation Buffer
- Bypass Schedule Range
- Bypass Suspension

Example: Facility requires 24-hour visitation buffer and has an active visit rule that allows Inmates to have two onsite visits per week. The facility can choose to override both the buffer policy and visit rule by choosing "Overrides" and the type of bypass while scheduling the visit.

Appointments scheduled in “Bypass” mode are not counted towards visitation rules but will be logged in the system logs.

- f. **Vender will provide a minimum of two (2) scheduling kiosks to be placed in the public access lobby at the main facility.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- g. **Vendor shall allow facility to manage remote and on-site video visitation, stations, visiting hours, time slots, and scheduling policies.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As the incumbent provider, Securus already has an established relationship with users who are familiar with our system, providing a seamless experience. This familiarity reduces the need for extensive training and allows for smoother transitions and continued operations without disruption. In 2025, Securus will have a major update to our visitation software. You’re Account Manager will be available to discuss these changes with you in the near future.

Sedgwick County authorized users **manage the authorizations for video sessions in the NextGen SCP system using Personal Visitation Lists (PVL).** You may configure the PVL for your facilities as either a Blocked List or Allowed List and your authorized users use the Inmate Profile Page in NextGen SCP to manage PVLs including adding, deleting, and editing entries. As changes are made, if a change impacts a scheduled video session, then the system alerts with a warning message. Each video guest’s Contact Profile page identifies any active entries on Inmate PVLs so the video guest knows which lists apply to them.

**Blocked List—a list of individuals who are prohibited from visiting with a designated Inmate.** At deployment this is the standard configuration and there is no limit on the number of individuals who may be blocked. This option gives you the ability to hide designated Inmate names from video guest searches and deliver custom messaging to video guests if a video session is blocked.

**Allowed List—a list of individuals who are approved for video sessions with a specifically designated Inmate.** You determine the maximum number of video guests per Inmate and they are only allowed video sessions with individuals on their PVL Allowed List. After the maximum number of entries is reached, Sedgwick County staff must delete an existing video guest before adding a new one. This type of list can be very restrictive but is useful for facilities that need the highest levels of control over video guests.

## Accessing the Inmate Personal Visitation List

The screenshot shows the Inmate Profile page for Attila Hun. The 'PVL' (Personal Visitation List) field is highlighted with a red box and labeled '0 active entries'. A blue callout box with an arrow points to this field, containing the text: "Click 'active entries' to view the inmate PVL." The page also displays various settings for calls and visitations, such as '3-way Calling Detection' and 'Maximum Call Duration'.

The PVL feature indicates the number of current active PVL entries. Authorized Sedgwick County users can manage—add, edit, or delete—PVL entries for Inmates on the Inmate Profile page. Changes to the Inmate PVL prompt a warning to appear, notifying the Sedgwick County user if any previously scheduled appointments violate the change in PVL.

## Impacted Sessions Warning

The 'IMPACTED VISITS' warning dialog box displays the following information:

**3** Previously Scheduled Appointments are in violation of this change

Visit ID	Visit Date/Time	Duration	Inmate	Visitor Type	Visitor	Relationship
100000442	10/24/2018 07:30 pm CDT	15	[Redacted]	NG Visitor	[Redacted]	Facility Admin
100000466	10/25/2018 07:15 am CDT	10	[Redacted]	NG Visitor	[Redacted]	Facility Admin
100000467	10/24/2018 10:45 am CDT	15	[Redacted]	Home User	[Redacted]	Aunt

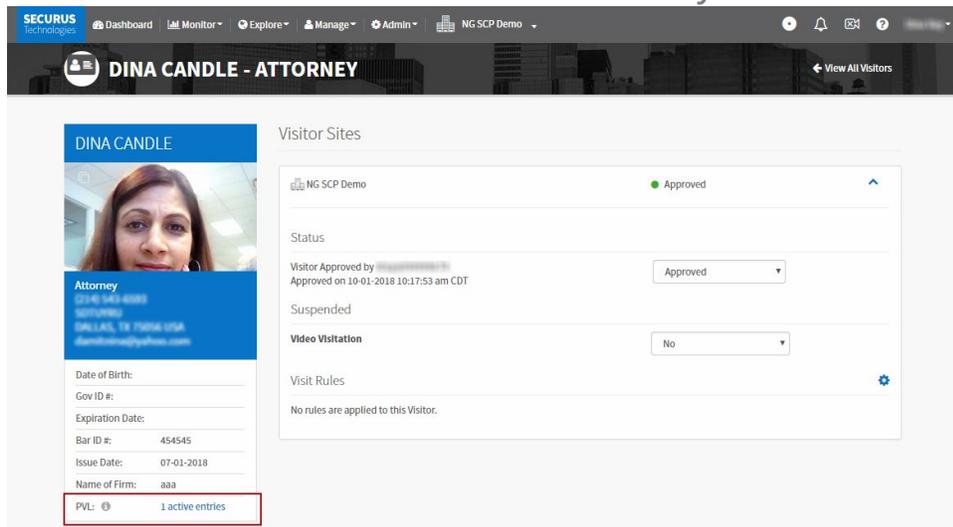
How would you like the system to handle impacted visits?

- Move visits that can be moved and **CANCEL** others.
- Move visits that can be moved and **DO NOT CANCEL** others.

A blue callout box with an arrow points to the second option, containing the text: "Select an option".

The guest's Contact Profile page also identifies any active entries on an Inmate's PVL. When the Contact Profile page has an active entry, that means the guest has been listed on an Inmate's PVL. Click the "active entries" link on the profile page to see on which Inmate PVL the guest appears. In the following example, the guest appears on the PVL of one Inmate; when selected, the hyperlink opens a list which show the Inmate's information and PVL type.

### Contact Profile with PVL Entry



## Creating Rules

While in the Visit Rules section, click on "Create Visit Rule" to create a new Rule.

## Create a New Rule

From here, you will define a rule name, and configure the following fields:

- **Status:** Active or inactive
- **Visit Rule Settings:** select the date for the rule to start and stop.
- **Visitor Types:** Home user, attorney, unregistered visitor, visitor
- **Visit Type:**
  - Onsite: Standard on-site visit
  - Remote: Applies to both friends & family home user and attorney home user
- **Rule Reset:** Daily, weekly, or monthly
- **Rule Applied On:** Apply the rule to a specific location

Users create a new rule without an initial association. The rule will not be in effect until there is, at least, one entity associated. Associations, in order of priority, are as follows:

- **Inmate Association:** Rule applies to a specific inmate or user
- **Visitor Association:** Rule applies to specific visitor
- **Terminal Association:** Rule applies to a specific terminal. \*
- **Terminal Group Association:** Rule applies to a specific location such as a pod. \*

- **Visitor Type Association:** Rule applies to every member of the user group to which the rule is associated
- **Site Association:** Rule applies to a specific Site. \*
- **Facility Association:** Rule applies to the entire facility.

*\*The behavior of rules is cumulative.*

Rules are prioritized based on the association level in which they are applied. For example, a visit rule applied to an Inmate (highest priority) takes higher priority than a rule associated with a site. This means that if there is a site-level rule that allows Inmates to have one onsite visit per month and an Inmate-level rule for a specific Inmate to have five onsite visits per month, the user level rule would take priority.

Example Visit Rule:

- Rule Name: 2 Visits per Week
- Visit Type: Onsite
- Quantity: 2
- Frequency: 1
- Duration: Week

Reads: 2 onsite visits per 1 week

If two rules with the same priority conflict, both rules will need to pass to schedule an appointment. An example of this conflict is an Inmate visit rule to allow one onsite visit per week and an Attorney Visitor Type visit rule that allows five onsite visits per week. Both rules must pass to schedule a visit.

### Associating Visit Rules

Enforcement of a Visit Rule requires association with a facility, site, terminal group, terminal, Inmate, visitor, or visitor type. Associations are easily applied while managing each of those.

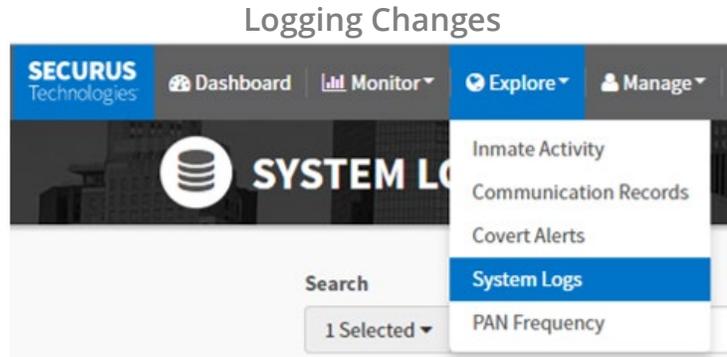
### Editing Visit Rules

Editing or deleting a visit rule can be accomplished through the Admin > Visit Rules menu.

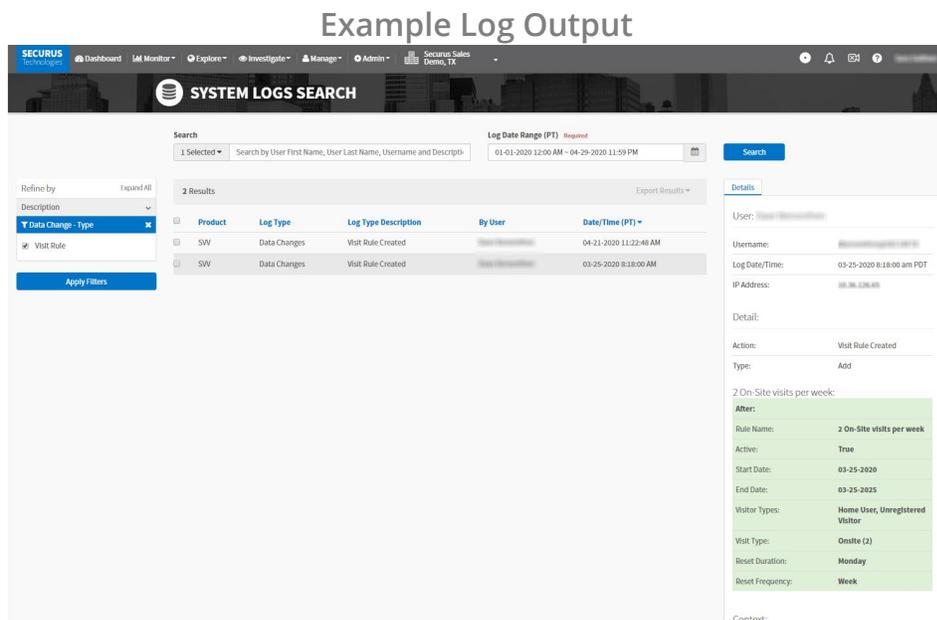
When editing a visit rule, you can modify all components of the rule. A popup showing the number of impacted sessions, if any, appears before saving a rule change. This prevents the unintentional cancellation of previously scheduled visits.

## Logging

The NextGen SCP logs all changes to Visit Rules, and this log is accessible from the Explore > System Logs menu.



Example log outputs include:



## Bypass Visitation Rules and Buffer

NextGen SCP allows authorized facility administrative users to bypass visit rules and visit buffers when scheduling appointments.

## Bypass Visitation Rules

The screenshot displays the 'CREATE VISIT' interface in the SECURUS Technologies system. The top navigation bar includes 'Dashboard', 'Monitor', 'Explore', 'Manage', 'Admin', and 'HG SCP Demo'. The main content area features a progress bar with six steps: Inmate, Visit Type (Onsite), Visitor, Visitor Details, Date & Time, and Confirm. Below the progress bar, there are fields for 'Visitor Terminal Group' (MRK Visitor Center), 'Visitor Terminal Group' (Helen VI Shared MPG), and 'Visit Options'. The 'Duration' field is set to 'Required' and 'Select'. The 'Overrides' dropdown menu is open, showing options: 'None Selected', 'All', 'Bypass Visitation Rules', 'Bypass Visitation Buffer', 'Bypass Schedule Range', and 'Bypass Suspension'. The 'Overrides' dropdown is circled in red.

Example: Facility requires 24-hour visitation buffer and has an active visit rule that allows Inmates to have two onsite visits per week. The facility can choose to override both the buffer policy and visit rule by choosing “Overrides” and the type of bypass while scheduling the visit.

Appointments scheduled in “Bypass” mode are not counted towards visitation rules but will be logged in the system logs.

- h. Vendor must store all recorded visits and make them available for review for a minimum of six (6) months.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- i. Visitation records will be kept for a minimum of five (5) years.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- j. All recordings must be stored off-site in a remote data center.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at Securus Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a

catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

**Unrivaled data resilience, scalability, and flexibility:** The Securus storage infrastructure has more than seven petabytes of storage space in each carrier-class data center. When these very large storage systems approach designated thresholds, Securus expands capacity. We won't run out of room and there is no limit on your data storage. The architecture of the Securus storage infrastructure makes all storage available to all servers on the network. The SAN/NAS solution delivers complete scalability for a facility's storage requirements and supports data migration from one storage device to another and the sharing of data among different servers in a network.

**Immediate online access to data anywhere at any time:** Typically, communication records are stored for seven years, but Securus works with Sedgwick County to define their optimal data retention policy. All data will be available until the earlier of the date the data retention policy date is reached or an agreed upon time after the contract terminates.

Securus uses a combination of an Oracle™ database and Elasticsearch® for storing CDRs. The Oracle database delivers economies of scale on easily managed grids, making it easier to reduce downtime with maximum availability, partition, and compress data to run queries faster, protect and audit data and use standby resources exclusively. Oracle simplifies the process of linking data in multiple tables—a key feature of a relational database management system. Storing data in multiple tables allows Securus to define relationships between the tables, as well as the applications that feed information to those tables. Elasticsearch is a distributed, RESTful search and analytics engine that provides Google™-like search capabilities for the Securus NextGen Platform. Elasticsearch stores a subset of CDRs from Oracle, allowing our customers to perform full-text queries with faster access.



The combination of our Data Centers and storage infrastructure provides a communications platform that is designed to meet your storage needs.

- **Scalable** to meet your required storage demands
- **Resistant** to local disasters through redundant and offsite storage facilities

- **Highly available** through the unique architecture and storage model design
- **Partitioned** and **compressed** to run queries faster
- **Secure, protected, and monitored** for total recall of data

k. Must include the option to manage the video visitation remotely in real time.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Authorized Sedgwick County users will manage the video system through the NextGen SCP® user interface (UI). They can access the UI through workstations at the facility or remotely from any internet-connected computer.

Securus offers Multi-Session Live Monitoring (MSM) through the NextGen SCP™. The Securus Video Connect™ (SVC) service MSM allows facility administrators to view a “slideshow” of all active video sessions. Up to 12 simultaneous sessions can be seen on the screen at one time—more than any other video provider. If there are more than 12 active video sessions at one time, the system will scroll through all active sessions, providing Sedgwick County management and control over inappropriate and suspicious behavior.

**Multi-Session Monitoring Window**



**How it Works**

MSM streams multiple, in-progress video sessions to allow the authorized user to monitor multiple sessions at the same time, which is ideal for facilities with a centralized monitoring room with multiple concurrent live visits.

A Sedgwick County user can configure the parameters to view all live visits according to their access credentials and preferences. The available parameters include:

- Visit type
- Visitor type
- Inmate terminal group or individual terminal

- Visitor terminal group or individual terminal

## Filter Parameters

The screenshot shows the SECURUS Multisession Videos interface. At the top, there is a navigation bar with options like Dashboard, Monitor, Explore, Investigate, Manage, Admin, and Marketing Next Gen Demo Site. Below this is a header for 'MULTISESSION VIDEOS' with a sub-header 'NG SCP Demo' and a dropdown menu for 'Marketing Next Gen Demo Site'. The main content area is titled 'Live Viewer Settings (Default)' and includes a 'Launch Multisession Monitor' button. The settings are organized into sections: 'Visit Type' (Onsite, Remote), 'Visitor Type' (Home User, Attorney, Unregistered Visitor, NG Visitor), and 'Preferences' (Session #: 4, Rotation Time: pause). The 'Terminal Group/Terminal' section is divided into 'Inmate' and 'Visitor' lists, both with checkboxes for selection. The Inmate list includes All, Pod A-3, Pod A-2, Pod A-1, Wintel A1, Wintel A2, Pod B, Wintel B2, Pod B-1, Pod B-2, and Wintel B1. The Visitor list includes All, MRK Visitor Center, MRK Visitation 1, MRK Visitation 2, MRK Visitation 3, MRK Attorney Visitation, Attorney 1, Attorney 2, Family Visitation, Family Visitation B, Family Visitation A, Visitor Terminal Group, EPMO Visitor Terminal 1, Helen VI Shared MPG, and Helen VI Shared Terminal 1. At the bottom, there is a 'Save these settings' checkbox, a 'Reset' button, and another 'Launch Multisession Monitor' button.

Sessions are displayed in the order in which they began, beginning in the upper left corner. For example, if a Sedgwick County facility has 12 sessions all scheduled to begin at 1:00 p.m., the first session in the upper left of the MSM window will be the visit where both the visitor and inmate joined first.

## Multi-Session Monitoring Window Details

The screenshot shows the Multi-Session Monitoring Window (MSM) interface. It displays a grid of 12 video feeds, each showing a different session. Below the grid, there are several controls and callouts:

- A volume adjustment control (represented by a speaker icon and a red 'X') with the text 'Volume adjustment (X)'.
- A session zoom control (represented by a plus sign icon) with the text 'Session zoom (+)'.
- A time remaining in session control (represented by a clock icon) with the text 'Time remaining in session (01:46:27)'.
- A screen rotation control (represented by a dropdown menu) with the text 'Screen rotation 60'.
- A manual navigation control (represented by left and right arrows) with the text 'Manually move the slideshow forward /'.
- A callout box with the text 'Adjust the slideshow screen rotation timer. Dropdown can be set to "Pause" in order to stop the slideshow from rotating to the next set of active visits.'

I. Vendor shall be responsible for all bandwidth required for internet video visitations.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus constantly monitors bandwidth usage, and will increase bandwidth if required to support uninterrupted Internet video visitations.

**3. Inmate Grievance Tracking**

a. Must have the ability to create grievance categories.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Communication Center**

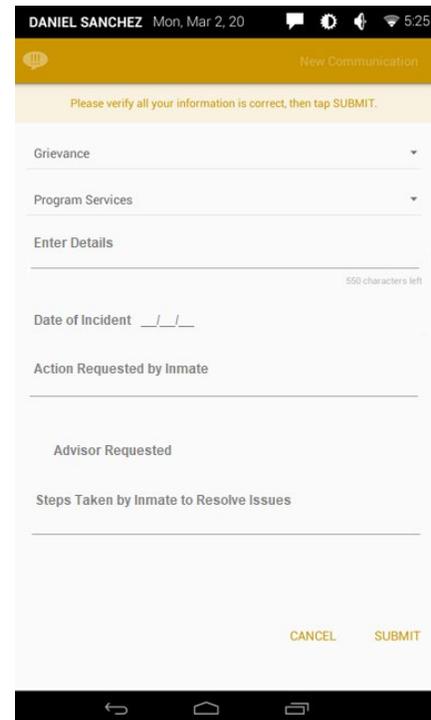
Sedgwick County can operate more efficiently and effectively by replacing manually processed paper forms from Inmates with an end-to-end electronic workflow through Securus' Communication Center. The Communication Center is a custom workflow tool that makes your grievance or form process paperless and allows Sedgwick County staff to process grievances. This application creates staff efficiencies and saves your prison/jail time, paper, and resources.

We lead the corrections industry with ever-improving technology and solutions, including the functionality for Inmates to submit and track various forms.

In addition to various forms, Securus can replicate any detailed problem resolution process that may require appeals, various levels of staff approvals and replies, and specific functionality so that the process supports Sedgwick County's policies.

Forms are submitted via the tablet and each unique submission receives a unique identifier to align the process between Inmate and staff. After submitting the form, the Inmate can track the form process, view replies, and perform other actions such as replying or appealing if specified.

From the staff side, each user has individual access rights so that they can view and respond to the specific forms. Within the system there are also several specific functionalities unique to the staff, such as comments and categorizations



not shown on the tablet, detailed search and reporting, and the option to add attachments.

### Facility Grievances Interface

Welcome mKunder1@SECUR.TXI-302805  
Last Login: 02/15/2021 9:48PM EST

Export to file Page 1 of 176

**Communications**

Assigned To Me (0)

New (12475)

Urgent (0)

Pending (7653)

Awaiting Response (1123)

Appealed (7)

Closed (425836)

Search

Reports

Communications Submitted Report

Create Communication

Communication Response Report

Print Communications

Restrict Inmate Form Use

**Inbox: New**

Filter by Forms: Inmate Letter Sort by: Date (Newest - Oldest) Filter by Location: All PermLocs Filter by Housing: All Housing

Ref.#:	<a href="#">AZA340000447159</a>	Inmate:	<a href="#">Gomez, Adan F.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">298103</a>	Subject:	Transfer Requests
Time Left:	27 d	Loc./Hou.:	A34 WG3B641B	Description:	See Subject Above
Ref.#:	<a href="#">AZM520000447158</a>	Inmate:	<a href="#">Munoz, Patrick</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">215284</a>	Subject:	Classification/Time Computation
Time Left:	27 d	Loc./Hou.:	M52 BL2FF14L	Description:	See Subject Above
Ref.#:	<a href="#">AZW050000447156</a>	Inmate:	<a href="#">Murabito, Cody W.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">316701</a>	Subject:	Banking
Time Left:	27 d	Loc./Hou.:	W05 HU02B20L	Description:	See Subject Above
Ref.#:	<a href="#">AZA340000447154</a>	Inmate:	<a href="#">Johnson, Jason M.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">161509</a>	Subject:	Safety
Time Left:	27 d	Loc./Hou.:	A34 WG3B537U	Description:	See Subject Above
Ref.#:	<a href="#">AZA340000447153</a>	Inmate:	<a href="#">Moreno, Albert A.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">343313</a>	Subject:	Transfer Requests
Time Left:	27 d	Loc./Hou.:	A34 WG3B641U	Description:	See Subject Above
Ref.#:	<a href="#">AZS060000447152</a>	Inmate:	<a href="#">Bejarano, Gilbert F.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">167825</a>	Subject:	Staff
Time Left:	27 d	Loc./Hou.:	S06 2401C12T	Description:	See Subject Above
Ref.#:	<a href="#">AZL210000447151</a>	Inmate:	<a href="#">Mendoza, Roy G.</a>	Form:	Inmate Letter
Created:	2/15/2021	ID#:	<a href="#">050778</a>	Subject:	Banking
Time Left:	27 d	Loc./Hou.:	L21 HU3A511L	Description:	See Subject Above

Prior to turning on any form, Securus will provide detailed training to both Inmates and staff, as desired. User guides can also be provided—as needed—to assist the various staff members using the system.

Overall, the top benefits of moving to the Securus digital problem resolution form include:

- Reduced staff time to track down and follow up in person on form progress. Overall, this saves Sedgwick County both money and time.
- Additional access for all Inmates via the tablet, including those using the free option, so they can submit over Wi-Fi
- Enhanced auditing of all system users for increased staff and Inmate accountability
- Enhanced tracking of a form throughout the process, from its submission to the time the form is closed
- Detailed reporting options with multiple ad hoc report options within our tools; Securus will also work closely with Sedgwick County to create customizable reports and dashboards to present the latest information in an easily accessible manner
- Customizable to allow for all forms and processes to fit into the solution

## Functional Overview

The Communication Center electronically processes a **wide variety of forms and communications submitted by Inmates.**

At a summary level, it provides the following functions:

- Form tools to create and manage multiple form types, each with its own customized workflow
- A user interface for Inmates to:
  - View a list of available form types for completion
  - Complete and submit a form type
  - View a list of their submitted forms and their statuses
  - View the resolution provided to a specific form and either Accept or Appeal the resolution
- An intuitive user interface for facility staff to:
  - View forms awaiting their action
  - Read and assign a form to another staff member for resolution
  - Request more information from the Inmate about a submission
  - Provide a resolution to a submitted form back to the Inmate
  - Establish velocity restrictions to limit form submission abuse
- Options to allow appeal levels to the workflow
- The ability for staff supervisors to:
  - Receive reports of the volumes and progress of forms through the workflow
  - Receive data charts representing age of forms currently in the workflow
  - Assign staff members to process specific forms
- An audit trail of all actions and form responses in the workflow
- Storage and retention of all forms

## Application Overview

The Communication Center allows Sedgwick County to replicate their existing paper forms in an electronic format.

Examples of forms include the following:

- General Grievance
- General Request
- Anonymous Grievance
- Request medications
- Request Law Library Access
- Request Sick Call
- Tablet Self-Help

### Form Capabilities

Key form capabilities include the following:

- Text fields are automatically filled using the NextGen SCP data, e.g., Custody Account Number
- Text fields entered by the Inmate
- Text fields entered by facility staff that can be configured to be hidden or viewable by Inmate
- Check boxes and other multi-select tools configurable by form
- Pre-formatted styles used to set the fields' location and format on the form
- Work-flow unique to the form type
- A General Grievance could have a workflow with multiple Appeal Levels, while a request for Law Library Access could have no Appeal level

### *Authenticated and Anonymous Forms*

#### Authenticated Forms

Authenticated Forms require an Inmate to log in prior to completing the form. The Grievance application attaches the Inmate's identity to the form for the visibility of facility staff. Optionally, Inmates can be required to re-authenticate to submit forms.

#### Anonymous Forms

An “anonymous form” does not require the Inmate to log in to the Inmate Forms and Grievances Application. The Inmate Forms and Grievances application does not attach the Inmate’s identity to the form to protect Inmate from possible recrimination. Anonymous forms have no means by which the Inmate may protest (escalate) the resolution of the form. Therefore, anonymous forms cannot have escalation levels.

Because anonymous forms have a simpler workflow than authenticated forms, they can be used as a light-weight processing of forms. Anonymous forms could be used to capture and process simple requests that do not need a response to be sent back to the Inmate.

Because the Forms and Grievances Application does not track the identity of the Inmate submitting an Anonymous form, the form can ask the Inmate to provide their name and/or custody account number.

Anonymous forms can be accessed by Inmates whose PINs are inactive and are restricted from using the phone system.

#### *Appeals/Escalations*

One or more appeal or escalation levels can be configured for each form. Simple requests typically do not have appeal levels configured. Formal grievance forms can have one or more levels depending on the facility’s existing grievance process.

#### *Velocity Restrictions per Form Type*

Adjustable velocity restrictions limit the number of times that an Inmate can submit a particular form to minimize abuse. After the limit has been reached, the application blocks the Inmate from creating more forms of that type until the next time interval.

#### *Form Categories*

Form categories provide users the ability to categorize the forms listed on the Inmate Forms and Grievance application.

#### *Auto Resolve Capability*

Auto-Resolve is a configuration that allows a form to automatically resolve itself if an Inmate is either released or transferred from the facility prior to the completion of the form.

### **b. Must allow for a multi-tiered appeal process.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

One or more appeal or escalation levels can be configured for each form. Simple requests typically do not have appeal levels configured. Formal grievance forms can have one or more levels depending on the facility's existing grievance process.

- c. **Must have the ability to set reply thresholds and have the capability to alert staff if a grievance remains unanswered.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Communication Center has the ability to set reply thresholds and alert staff if a grievance remains unanswered. Please reference response to requirement 3(a).

- d. **Must maintain records of all grievances for a minimum of five (5) years.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Grievance records are not deleted and are kept for the life of your contract with Securus. At the end of the contract, you can download grievance information for storage and archive.

- e. **Must be a web-based system that allows staff to log in from any station to answer grievances.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Communication Center is web-based system that allows staff to log in from any station to optimize workflow and answer grievances.

- f. **Must be available for inmates to access via a wall mounted kiosk.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Inmates access Communication Center application through tablets and wall mounted kiosks.

- g. **Must have the ability to search for grievances by inmate name, grievance category, location, and individual grievance number.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The system allows searching for grievances by inmate name, grievance category, location, and individual grievance name. Please reference response to requirement 3(a) for more information.

- h. Must have the capability to allow staff to reassign grievances with a notes field, not viewable to inmates.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Communication Center has the capability to allow staff to reassign grievances and has notes field that is not viewable to inmates.

## **4. Digital Mail**

- a. Must have the ability to scan all non-privileged mail off site.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

These days, agencies like yours are seeing deadly substances like Suboxone and Fentanyl penetrating facilities disguised as paper, stamps, colored drawings, and more. Often, these toxic drugs are nearly impossible to detect by mailroom personnel—putting staff and population at risk, for accidental exposure.

Along with the safety and security hurdles, agencies also need to increase operational efficiencies due to labor shortages, and budget constraints.

## **Digital Mail Center**

We understand that reducing risks and boosting your facilities' operational efficiencies are among your top priorities. That's why we developed a comprehensive mailroom operations product: Securus Digital Mail Center (DMC®). DMC can play an integral role in helping you solve your agency's biggest hurdles—safety and security, labor shortages, and budget constraints.

### **DMC's streamlined & Securus-owned process**

With DMC, we take on the administrative and safety burden of evaluating your facilities' postal mail. All *non-privileged* postal mail will be forwarded to a Sedgwick County-assigned P.O. Box, where our team receives the mail and delivers it to our dedicated processing center. From there, our certified mail processing staff:

- Scans and transcribes all postal mail envelopes and contents through Optical Character Recognition (OCR) software

- Evaluates mail for illegal substances and contraband
- Investigates electronic transcripts for words identified on Sedgwick County's word watch list, and sort flagged communications into a specific review folder for further assessment
- Upload it to the Sedgwick County mail portal, for review and distribution to your incarcerated population via tablets and/or terminals

Mail is collected each morning when the USPS Business Mail Entry Unit is open and operational (Monday – Friday), and then processed and digitally delivered within 48 hours of receipt from the post office. Mail that is rejected is returned to the sender as long as a correct return address is provided.



**b. Must be able to identify name and address of sender.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

***Mail received from an attorney's office or other private/privileged establishments will not be received for processing.*** Any legal and/or privileged items received will be marked with the reason for rejection and returned to the sender. Items that are legal in nature can be mailed directly to the agency where agency staff will receive and distribute those items to the intended inmate.

**c. Must be able to convert all non-privileged mail to a digital format available for inmate viewing via wall mounted kiosk.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

With DMC, we take on the administrative and safety burden of evaluating your facilities' postal mail. All ***non-privileged*** postal mail will be forwarded to a Sedgwick County-assigned P.O. Box, where our team receives the mail and delivers it to our dedicated processing center. From there, our certified mail processing staff:

- Scans and transcribes all postal mail envelopes and contents through Optical Character Recognition (OCR) software

- Evaluates mail for illegal substances and contraband
- Investigates electronic transcripts for words identified on Sedgwick County's word watch list, and sort flagged communications into a specific review folder for further assessment
- Upload it to the Sedgwick County mail portal, for review and distribution to your incarcerated population via tablets and/or terminals

**d. Scanned mail will not be available to be viewed by inmates until reviewed and approved by Sedgwick County staff.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our DMC solution offers an integrated solution with a mail management portal. In this portal, you can review, track, and approve all incarcerated postal mail that enters your facility.

Here's how the DMC mail management portal works:

1. We deliver an English transcription of the scanned envelope and all mail contents to the agency queue for you to review and approve
2. You review the mail items and any mail contents and approve or deny the piece(s) for delivery
3. If approved, the mail is automatically distributed directly to the intended inmate via the eMessaging application available on their tablet or facility terminals
4. The DMC system automatically logs all mail activity

Each mail item is assigned a unique identifier and is automatically delivered to the agency portal for review and approval. From the agency portal, you have complete control over what mail items are approved or denied. You can approve/deny individual pages, photos, or other specific pieces of mail. The agency portal also allows you to choose individual mail items, or all mail items for bulk approval or denial.

**e. Must include an option to send and receive e-messages.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## eMessaging



Securus eMessaging™ is the most widely used messaging platform in the corrections industry. Sedgwick County has control of who uses the system and what messages are permitted.

- Facilitates electronic communication at no cost to Sedgwick County
- Increases investigative data and analysis with all digital review
- Implements easily with existing facility network connectivity and hardware
- Prevents inmates from sending messages to other inmates at your facility or any other facility

**Inexpensive, user-friendly options to maintain connections without sacrificing security:** Securus eMessaging™ is an easy way for friends and family to stay in touch using the free Securus App or on our website. Both provide a high-level of security for communication entering your facility. Friends and family purchase stamps to send eMessages with the option of using an additional stamp to attach an eCard, photo, or video.

**Stamp Packages** may be purchased by an inmate using their Securus Debit Account and by friends and family using a credit or debit card. After the Stamp Packages are purchased, they may be used to send messages, transfer stamps to an inmate for their use, and to pre-pay for a return message from an Inmate.

**Snap n' Send™** gives friends and family a tool to send just a photo for one stamp. It's an easy way for friends and family to share photos from their phone or photos snapped at family celebrations, kids sporting events, or just because.

**eCards**, like traditional greeting cards, celebrate life events and holidays with pre-worded, un-editable messages. An inmate or friends and family may send eCards for the cost of just one stamp.

**VideoGrams** are a convenient way to send 30 second videos from the Securus App for Android and iOS mobile devices. The Securus App automatically crops longer videos with no extra steps.



## eMessaging Dashboard

**Reduced administrative burden:** Securus eMessaging™ is an advanced, digital investigation option that reduces Sedgwick County administrative burden while increasing your control over communication and content. Our centralized, proprietary platform is managed wholly within the United States and can be configured to match Sedgwick County goals. The NextGen SCP is where you choose the level of review by choosing security controls. Then as eMessages are processed, if none of your security controls are triggered, the eMessages “Auto Release.” If your security controls are triggered, then you have an opportunity to review the flags and approve/reject the message. Each eMessage that is rejected generates an automatic, free message to the inmate or family and friend sender advising that their message was not forwarded with a stated reason.

**Minimize time and maximize results with automated screening:** The NextGen SCP allows you to view and analyze the complete mail history of any sender. Intuitive reporting and views provide a complete message history by inmate, and the ability to search messages by inmate, family and friend, date, specific message, and word filter list. Use this tool for timely identification and evaluation of big-picture communication issues so you can proactively address.

All messages and photos are retained for the term of the contract, even if they are rejected or deleted by recipients. An additional benefit--as electronic communication increases, you can redeploy mailroom resources to other agency tasks.

**Photo Review:** Photo Review is efficient using the NextGen SCP’s Photo Review Folder. If photos are outside Sedgwick County photo policy, you may remove them (individually or as a group) from the message while allowing the message and acceptable photos to be delivered. The sender receives a notification that a photo was removed. All photos that were removed remain associated to the message and are accessible to Sedgwick County. The NextGen SCP captures both the date and the staff member for each removed photo.

**Word Watch:** The word watch filters automatically screen and flag for review all incoming and outgoing messages that include a word on the Sedgwick County Word Watch List. The flagged words will appear in red at the top of the message for fast review. You may modify the Word Watch List at any time to align with trends in coded speech phrases or buzz words.

## Word Watch Filters Flagged Words in eMessaging

LETTER ID 1234567

**Inmate Name :** JAMES MEEKS  
**Inmate ID :** 1234567  
**Housing :** BTCE09 19  
**Date :** 07/18/2023 2:53PM EST  
**Customer :** volletta larson  
**Customer ID :** 1234567  
**Word(s) Found :**

- weed
- weed
- major
- parole

<a href="#">Approve Letter</a>
<a href="#">Send To Sent To Security</a>
<a href="#">Returned To Customer</a>
<a href="#">Send To Censored</a>
<a href="#">Mail History</a>
<a href="#">Relocate Letter</a>

**Attachment(s) :**

[Click here](#) to discard letter content. Discarded letters will be saved in the Discarded Material Bucket

a lil bro whats good in there got that mst of a in fo for u gotta remember i know those books so tell mom to tell me n ill show her for u ok . im cool just nworking n we trying to set up a video visit for u bro i wanna c u .she on tha phone now i think they sayin they dont have it but mom checkin wit somone eles now . but how long b 4 u home stud ? im waiting ?????u cool u get that \$ mom sent ? wanna write sum broads i know u cool on that but hey never enough !!!!!!! lol im gettin it heavy out here as far as hoes go but not enough \$ bro . i finnaly popped tony off about that smoking weed it got bad for a hot sec but u know iwant tha best for him n he know it to ill holla at u more on that on tha phone . allah is steady blessin its slow but its going i aint had to do no major dirt so to me its all been a dream except my right hand aint here i really need u tane i cant figure this out i need a solid lick to put me on for tha \$ i need to get my

**Watch Lists** allow Sedgwick County to flag for review all communications from designated individuals in your population and/or their friends and family. You may modify the Watch List at any time.

**Emessaging Suspension:** This feature allows you to stop all communications to any individual using the system. Pop-up notifications alert senders if they are suspended or if the intended recipient is suspended. Each suspension and reactivation action for an inmate is logged with staff name, date, and reason for the status change; suspensions may be modified at any time.

### Inmate Access

Using a Securus Tablet or other device, an inmate can retrieve eMessages sent by friends and family. At log-in, there is an indicator that shows an eMessage is available and once opened, it clearly shows if there is a photo, eCard, or video attached. The inmate can reply to the sender by using a stamp they purchased using their Securus Debit Account, a stamp that was transferred to them, or a stamp that was paid for by the sender and attached to the incoming eMessage.

All eMessages, photos, eCards, and VideoGrams are displayed on the terminal or tablet in an eMessage inbox with no paper distribution. There is no Draft folder for the inmate and the Sent folder may be deactivated by Sedgwick County.

f. All digital mail records will be maintained for review for a minimum of five (5) years.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Digital mail records are not deleted and are kept for the life of your contract with Securus.

g. Must have the ability to manage users and restrict access for inmates and outside parties due to non-compliance with facility rules or court orders.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Investigate and monitor facility mail, build your intelligence database, flag mail, create watch lists, and more:** With safety and security a top priority, for Sedgwick County, we developed DMC to support your agency's intelligence efforts. DMC stores all information associated with the physical mail piece including: a Securus-assigned unique identifier, the sender's name, time, date, address, and content, for the life of your contract with Securus. This long-term archive capability allows you to build an investigative intelligence database that's not possible through standard physical mail processing.

The mail portal also offers additional investigative and monitoring functions, including:

- The ability to create customized watch lists to flag postal mail for specific words (Word Alert)
- Flag specific incarcerated recipients and/or external senders for additional review
- Define mail retention periods for scanned physical mail. (90-day default)
- Audit and track all mail activity
- Search for specific mail items
- Export mail documents from a search result for investigative documentation

After the mail is scanned, Securus stores the mail on behalf of the agency based on the agency's defined mail retention period. By default, Securus stores all mail for 90 days. After the retention period has expired, the mail is destroyed.

Also, mail that contains words identified on your agency's customizable watch list is flagged so you can send flagged mail to security for further evaluation prior to approval/denial. Our DMC solution allows you to control what inmates can receive in their mail, and what mail external senders can send. With the mail portal, you can flag specific senders and recipients, and require that mail from those identified parties undergo additional levels of review.

## 5. Tablets

- a. **Tablets will be provided at a 1:1 ratio to inmates housed at the Annex Facility only (approximately 180).**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus will provide tables at a 1:1 ratio to inmates housed at the Annex Facility only.

- b. **Must contain free content allowed to be accessed by all inmates.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The **free** Personal Tablet provides inmates immediate access to free content, including communication, self-help, and education applications. Our free programs also include access to religious content, and post-incarceration employment applications. These free services are proven to reduce recidivism and have assisted inmates in rejoining society. For a small fee, an inmate may choose the Personal+ option on the Make Mine app to rent or purchase premium content. Premium content includes access to agency-approved media and entertainment.

- c. **All fees must be consistent with all federal, state, and local laws.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

All fees are consistent with federal, state, local laws, and new MWRA regulations.

- d. **Must provide staff tablets with the ability to manage inmate usage.**

## **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. NEXT GEN OFFICER TABLET**

Securus is uniquely positioned to solve the technical challenges faced by customers in the correctional landscape. Our new Officer T80 tablet stands as a beacon of innovation and precision, addressing facility needs with best-in-class efficiency and foresight.

### **Achieve Unmatched Flexibility and Control.**

Our T80 tablet ecosystem offers unparalleled flexibility and control, allowing seamless integration of Securus applications alongside apps from a managed, private Google Play store. You can customize each tablet to meet your agency's specific needs, with support for multiple user profiles, as well as connectivity options.

### **Get Google-Certified Security.**

By transitioning our officer tablet to the Android Enterprise platform certified by Google, Securus is able to provide tablet security with the highest security standards. Using a device that is Android Enterprise-certified provides a robust and comprehensive security framework backed by Google's safety expertise. From over-the-air patches to malware detection, our Officer T80 tablet protects sensitive data, mitigates risk, and maintains a secure environment that helps you keep your staff and population safe.

### **Experience Cutting-Edge Hardware**

You'll hold the latest in corrections tablet technology in your hands with our Officer T80 tablet. Featuring an 8-inch HD touchscreen, 3GB of RAM, 32GB of storage, extended battery life, and built-in GPS, our Officer T80 device is five times faster than our previous model and is built to withstand the demands of modern correctional facilities.

What's more, our T80 officer tablet is tailored to help you solve business critical issues by bridging the gap between technology, staffing and operations.

Here's how our latest offer tablet solution will transform the way you work.

### **Add Flexibility to How You Administer Your Tablet Program.**

Since our T80 officer tablets leverage an LTE connection, you can manage any active device that's part of your tablet program without actually having to be connected to the local site. This means that you're able to control your devices from anywhere – your agency headquarters, inside a different facility, or even at home!

### **Streamline Operations.**

By offering you the ability to download apps available within our managed, private Google Play store, you can select the pertinent application solutions that help your staff handle policy changes, signatures, incident reporting and other critical tasks. Our T80 officer tablet helps optimize operational workflows, saving you time and resources.

### **Reduce Technology Costs.**

Say goodbye to multiple devices cluttering up your workspace. The T80 officer tablet serves as a comprehensive solution, eliminating the need for supplementary administrative technology such as computers, smart devices, and full workstation setups in housing units. This consolidation reduces the budget required for you to offer a full-service technology suite.

### **Simplify Tech Management.**

With automatic over-the-air updates and robust security management directly from Google, maintaining the T80 officer tablet is effortless. Our full-service tech management solution ensures your staff can focus on essential facility tasks without the burden of constant oversight across multiple devices.

### **Boost Employee Recruitment and Retention.**

By expanding the capabilities of the officer tablet to support non-Securus applications, we empower you to select apps for your staff from a wide array of Google-ready apps we've made available in our managed store. Our T80 officer tablet gives you the ability to enhance staff education and training programs while fostering a supportive work environment.

Revolutionize your correctional operations with the Securus T80 officer tablet. This innovative technology powerhouse will elevate your facility's performance and security standards to help you achieve organizational goals... with a click.

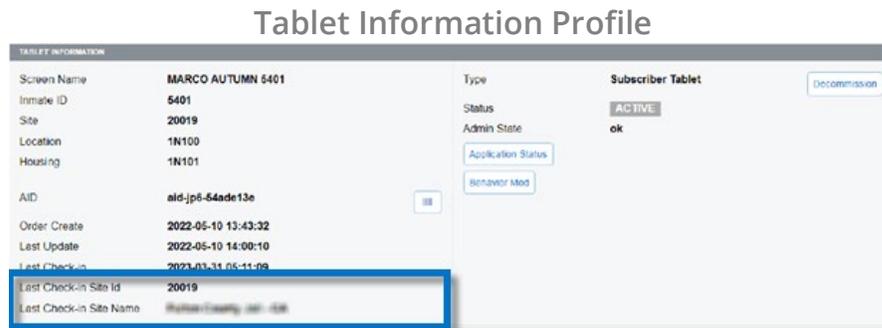
### **SubManager App**

The SubManager Application is used by agency staff for the command and control of tablets deployed at the agency. The application can be perform, but is not limited to, the following functions.

- Tablet Lookup
- Check inmate eligibility
- Assign/Reassign

- Availability Restrictions
- Behavior Modification
- Tablet Messages
- Inventory

Every tablet has an information profile identifying the user of the tablet, the inmate ID, the site location and ID, housing unit location, last usages, and permission status, as shown in the following image.



e. Must contain WIFI and have the ability to be updated wirelessly.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Tablets are able to connect to the secure Securus Wi-Fi network and obtain an IP address if it is recognized as an authorized device by the SLP. If a tablet is not known by the SLP, it will not be granted access to the wireless network and will be rendered useless for applications that require network connectivity.

Updates to EVOTAB Tablets are done wirelessly. These updates include virus protection, application updates/upgrades, and patches, with no need to sync to external hardware. The EVOTAB firmware includes the antivirus protection for the tablets, so there is no need for a separate anti-virus program to be installed. With any new firmware release, it includes updated anti-virus protection.

As we transition to EVOTAB we recommend using our **secure LTE solution**. This provides SIM based security, in an always on VPN that is always directly whitelisted with the carrier network to only route traffic to our data centers, allowing us to maintain full control of the connectivity and any breakout.

f. Tablets will not be equipped with a camera.

**SECURUS HAS READ, UNDERSTANDS, AND WILL PARTIALLY COMPLY.**

EVOTAB tablets come equipped with a camera; however this camera is only active for video visitation. The SVC application can be removed from the tablet interface.

- i. If a camera is built into the provided tablet it must have the ability to be disabled.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTAB cameras will only be active during video sessions. The SVC application can be removed from the tablet interface at Sedgwick County's discretion.

- g. Tablets will be replaced as needed at no cost to the county.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTABS will be replaced as needed at no cost to Sedgwick County.

- h. Tablets must be designed for use in a correctional facility with durable and tamper proof materials.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Unlock a new era with EVOTAB, the pinnacle of tablet innovation, designed solely for the corrections market. As the pioneer in our category, Securus has integrated industry-best hardware and tech-forward features to deliver a device that's redefining what it means to be *corrections grade* and to provide next-level support to your staff. EVOTAB is robust, secure, and user-friendly... revolutionizing the way your Correctional Officers will manage your tablet program and keep your facility safe.



**EVOTAB Conquers Tough Environments.**

While other tablets on the market may meet some durability and toughness criteria, our EVOTAB is specifically crafted for hardened spaces. Securus has engineered EVOTAB to withstand even the harshest situations.

- **Deters unauthorized access and intentional damage** with a single-mold, no-screw design and tamper-resistant assembly.
- **Resists dust and water** with IP52-rated tablet construction and an IP68-rated headphone jack, ensuring reliability and quality audio in even the most challenging conditions.
- **Provides safety from drops and impacts** with a TPU of shore hardness 85 type A and TPU bumpers that make cleaning the device easy and eliminate the need for additional protective cases.
- **Withstands high-frequency use** with a rugged design, including sculpted ribs providing improved grip and durability.

### **EVOTAB Improves Safety and Security.**

This tablet offers the most robust security and safety features available in the corrections technology market. We've designed our device with built-in, top-tier security features including tracking, chirping, and tamper detection alerts to help your staff be more efficient. EVOTAB:

- **Utilizes a proprietary, secure operating system** built off the Google-Certified Android Enterprise platform and backed by Google Security services.
- **Offers authorized device access** through the power button that doubles as a biometric fingerprint scanner to help prevent PIN sharing and serves as an alternative to facial/photo recognition verification.
- **Identifies unauthorized device tampering** with an audible "shriek alarm" when device interference is detected.
- **Mitigate against network tampering** with alerts sent directly to staff if networks are manipulated.
- **Locks devices down automatically** using a tamper circuit that bricks the tablet if the secure device enclosure is breached.
- **Delivers simple tablet tracking and monitoring** with built-in GPS functionality.
- **Helps you locate a tablet easily** by triggering an auditory alarm – even when the tablet is offline.
- **Safeguards against device fraud**, with no external ports, reducing the risk of connecting unauthorized cords or devices.
- **Controls features**, such as Securus Video Connect, are available within certain areas of your facility.

- **Connects to Officer T80 tablets** to provide seamless tablet monitoring and administration for your officers, enhancing safety and compliance.

### EVOTAB Delivers Tech-Forward Hardware.

This device brings you the latest in regulatory-compliant incarcerated tablet technology, including:

- **An improved user experience** with a large 8-inch HD, in-plane switch touchscreen display that makes engaging with tablet content more satisfying for your population.
- **More space for content** with 64 GB of storage (*two times* the storage capacity of our JP6s) so users can download more messages, photos, and media to their devices.
- **Top-speed tablet performance** with 3 GB of RAM – *five times* faster than our JP6s.
- **Enhanced tablet processing** with an Octa-Core central processing unit (CPU) chip.
- **Extended battery life** – up to 8 - 12 hours of constant usage.
- **Multiple connectivity options** through a local network and 4G LTE.
- **Tracking and controlling tablets** with Bluetooth, NFC and GPS.
- **Fully compatible with Officer T80 tablets** to provide an end-to-end solution that is customizable to your unique needs.



### EVOTAB in Action

How can EVOTAB help you mitigate risk and solve critical problems within your facility? Let's explore some common issues and how EVOTAB addresses them.

### **SCENARIO 1: Tablets can't withstand the corrections environment.**

**Problem:** Tablets aren't durable enough and are breaking down due to continuous use.

**Solution:** EVOTAB redefines *corrections-grade* technology and is engineered to withstand even the most challenging environments.

- The IP52-rated tablet construction and IP68-rated headphone jack make the EVOTAB dust- and water-resistant.
- A rugged design and sculpted ribs help improve grip, helping to prevent drops.
- TPU of shore hardness 85 Type A and TPU bumpers ensure the tablet is impact-safe without the need for a protective case.
- The single-mold, sealed design makes the tablet easy to clean.
- An improved SIM-shaped pogo pin eliminates confusion between charging ports and headphone jacks, preventing accidental device damage.

### **SCENARIO 2: Incarcerated individuals are physically damaging devices and using them inappropriately.**

**Problem:** People are tampering with tablets, trying to hide contraband inside them, using device parts as weapons, or using their power cables to charge contraband devices.

**Solution:** EVOTAB is built tough and is resistant to even the most extreme device tampering attempts.

- A single-mold, no-screw design makes device tampering unlikely.
- If tampering is detected, an audible "shriek alarm" will sound so your staff can quickly identify and confiscate the tablet.
- The tablet will brick itself and become unusable if the device enclosure is breached.
- A SIM-shaped pogo pin with intelligent power connection limits charging misuse and blocks the ability to charge contraband devices.

### **SCENARIO 3: Incarcerated individuals are attempting to manipulate the tablet software or the network.**

**Problem:** People are trying to hack the tablet operating system or leverage a Wi-Fi connection to access the internet or participate in nefarious activity.

**Solution:** EVOTAB leverages multi-layered operating system security protocols.

- Our proprietary OS is built off the Google Certified Android Enterprise platform, using the highest safety and security standards to mitigate hacking.
- EVOTAB delivers advanced defense against vulnerabilities through anti-exploitation protocols.
- Devices are backed by Google Security services that continuously scan and block malware threats.
- If network tampering is detected, your staff will receive automatic alert notifications.

#### **SCENARIO 4: Tablets are lost or stolen.**

**Problem:** Tablets are missing from inventory, so people are intentionally hiding them, they have been lost, or they have been stolen.

**Solution:** EVOTAB makes it easy for your staff to locate tablets.

- Built-in Bluetooth, NFC and GPS allow your staff to track, in real-time, the exact location of every tablet in your program.
- Staff can trigger an auditory alarm to help locate missing tablets.
- GPS and alarms function even when a tablet is offline.

#### **SCENARIO 5: Incarcerated individuals are sharing credentials and devices.**

**Problem:** Multiple people are using the same login and tablet, making it difficult for staff to manage authorized device access.

**Solution:** EVOTAB security ensures that only the user who is assigned to a tablet can access it.

- The power button doubles as a biometric fingerprint scanner to mitigate against PIN sharing.
- The fingerprint scanner also provides an alternative to facial recognition verification.

EVOTAB empowers your corrections staff *and* your incarcerated population with secure, reliable technology that supports rehabilitation and revolutionizes the industry.

We invite you to join us in shaping the future of corrections technology... exclusively with EVOTAB.

- i. **Tablets must have a location feature with an audible notification to assist in finding lost or hidden tablets.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**SCENARIO 4: Tablets are lost or stolen.**

**Problem:** Tablets are missing from inventory, so people are intentionally hiding them, they have been lost, or they have been stolen.

**Solution:** EVOTAB makes it easy for your staff to locate tablets.

- Built-in Bluetooth, NFC and GPS allow your staff to track, in real-time, the exact location of every tablet in your program.
- Staff can trigger an auditory alarm to help locate missing tablets.
- GPS and alarms function even when a tablet is offline.

## 6. Miscellaneous

- a. **The successful vendor, will develop a mutually agreeable fault hierarchy rating system. Corresponding service time interval that requires a service representative to be on-site not later than 24 hours after receipt of a call for service. This is to correct any malfunction or loss of service to any part of the system or the system as a whole.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

If Sedgwick County experiences a loss of service or malfunction, it will be due to a lack of an internet connection. Securus will notify Sedgwick County when any maintenance / updates occur affecting the availability of being able to log into the system. There is no physical system equipment on-site that will require maintenance. An on-site technician will be able to assist with tablet issues.

- b. **Wall mounted kiosks shall have the ability to: conduct voice calls, video visitation, view digital mail, manage inmate grievances, and access any other value adding services provided by the vendor.**

## **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. -**

Wall mounted kiosks will have the ability to: conduct voice calls, video visitation, view digital mail, manage inmate grievances, and access any other value adding services provided by Securus.

## **EVOTAB Terminal**



Concept Only, Design and Product Not Final

### **Software features include:**

- Current and future EVOTAB apps and functions are supported, including VRS, SVC, outbound Videograms, and mirrors the same, familiar log-in process as the EVOTAB Tablet.
- Portrait mode is available for all applications while remaining ADA compliant.
- Customizable permissions allow facilities to limit specific applications or disable the entire terminal.
- Manage scheduled video visitations with the Conflict Management feature to facilitate transitioning inmates off a terminal before a scheduled video visitation is to start. Controls are configurable based on facility preference.

**Providing easy-to-access and easy-to-maintain technology solutions:** With our solutions, onsite Securus administrators can replace terminals while maintaining security standards. Plus, with 24x7x365 secure monitoring supported by Securus staff, our solutions are safe, reliable, and protected.

**c. Wall mounted kiosks must contain the following items:**

**i. Minimum of a 16" touch screen monitor.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL PARTIALLY COMPLY.**

The new EVOTAB wall mounted kiosk offers a 8" HD color screen display that is ADA compliant.

**ii. Integrated high-definition camera**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTAB wall mounted kiosks are integrated with a high definition camera.

**iii. Institutionally approved handset**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTAB wall mounted kiosks include an institutionally approved handset.

**iv. Institutionally approved enclosure to prevent tampering.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTAB wall mounted kiosks include an institutionally approved enclosure to prevent tampering.

**d. Vendor must supply a centralized platform to monitor or review all inmate communications.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Industry-leading technology with input from corrections and law**

**enforcement partners:** The NextGen SCP is an integrated software platform for managing, researching, monitoring, investigating, and exporting information through Securus products and services. Built from the ground up with input from corrections and law enforcement professionals, Securus NextGen SCP has

the industry-leading technology, features, and functionality you need to manage communications and support investigations at your facilities. Securus' Video Connect platform will undergo a major update in 2025. Please talk with your Account Manager for more details about this plan.

- Integrated interface to manage communications and investigations
- Reliable network and secure data storage with built-in redundancy

<b>Securus NextGen SCP Key Features</b>
<p>Refined User Interface</p> <ul style="list-style-type: none"> <li>• Easily maneuver with action-based navigation</li> <li>• Use Google-like single entry search fields</li> <li>• Get more information with less effort in a shorter amount of time</li> </ul>
<p>Custom Dashboard Configurations for Easy Data Viewing at Login</p> <ul style="list-style-type: none"> <li>• See summary overview of facility communications immediately</li> <li>• Quick access to BNA and PAN frequency search functionality</li> <li>• Access upcoming video sessions</li> </ul>
<p>Improved Records Search Experience</p> <ul style="list-style-type: none"> <li>• Increase the speed from request to data reducing your investigative time</li> <li>• Get multi-product results with a single search</li> <li>• Integrated backend technologies analyze and store data efficiently for fast access</li> <li>• Run reports in the background while continuing to work and get notice when ready</li> </ul>
<p>Comprehensive Population Oversight</p> <ul style="list-style-type: none"> <li>• A convenient activity stream shows all past, present, and future communication events</li> <li>• Manage settings and suspensions for calls, video, and other products independently</li> </ul>

#### Single Platform to Manage Calls, Video, and Visits

- Use the Contact Profile page to view visitor information and manage visits
- Set up facility and site level approvals custom-designed for your needs
- Manage visit approvals flexibly at first visit only, every visit, or automatically

#### Security and Access Management Flexibility

- Provide users with access and edit rights only to information needed to do their job
- Easily craft custom task-based permissions for admin. and investigative teams
- Protect your facility access with required strong passwords and regular updates
- Provide facility affiliated personnel with access to video sessions

**Data, security, and control over communications:** NextGen SCP gives you fast and efficient access to communication data, increased security, unparalleled control over Inmate communications, and real-time alerts. Your data gathering systems will work together and deliver key insights in one place. NextGen SCP is entirely web-based, so your authorized users may access the system at any time, from any location.

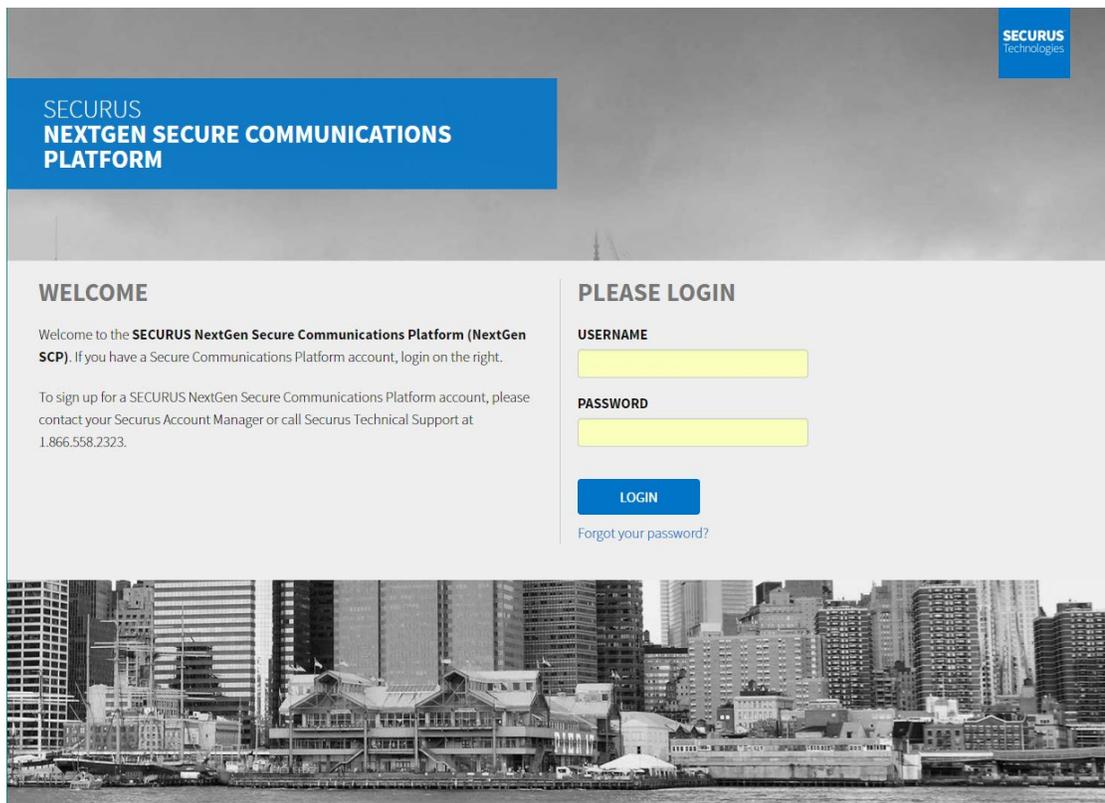
**Backed by high-performance data center:** The back-end equipment for NextGen SCP is housed in a carrier-class, commercial-grade data center built to the latest technology standards. This includes all hardware and software, fraud controls, investigative features, user utilities, call/video processing, and communication event recording. The hardware and software components adapt to the changing needs of your facility's operations, and can monitor, record, and block/unblock communication, and generate reports in real time.

Premise equipment includes Adtran and Cisco routers and IADs (Integrated Access Devices) that convert VoIP to analog signals for the Securus systems. Securus-provided workstations are the latest generation Dell processors, with Dell flat screen monitors and HP inkjet printers. Netgear or Cisco switches connect workstations to the Securus network.

**Corrections-grade equipment to withstand harsh conditions:** The traditional telephones are shock-resistant correctional facility-grade equipment that are hearing aid-compatible and mounted to ADA standards, where applicable. The video session terminals are correctional facility-grade with tamper-proof steel enclosures, shatterproof touchscreens, a high-resolution video camera with integrated lighting,

and heavy, molded plastic handset with an armor-reinforced cord for audio communication.

**Real-time administrative control over communications:** Securus NextGen SCP, as a single-point-access user interface, gives Sedgwick County complete control over your systems in a simple, reliable, secure environment. The system adapts to your facilities and operations, rather than requiring you to conform to the software. Authorized users can apply settings and configurations in real time to turn on a device/terminal, restrict a device/terminal, change a blocked number, administer approvals for call and video lists, and turn on/off features and applications.



**Secure, any time/anywhere access:** To access the Securus NextGen SCP interface, your users will open a Chrome™ browser and launch the URL: <https://ngscp.securustech.net/login>. After entering a valid username and password, all integrated features are accessed with just the click of a mouse. Securus NextGen SCP™ is protected by SSL (secure socket layer) security, which uses the same security protocols that banks use for establishing a connection for customer online banking.

**Information at your fingertips:** The Securus NextGen SCP dashboard is a configurable landing page giving quick access to often-used functions and a proactive overview of your communication systems in user-specific widgets. The

Announcement Panel is where Securus posts notices about system maintenance, feature enhancements, and training opportunities.

Sedgwick County **control over access rights:** Assign access rights to each user role to control access based on the facility's security clearance objectives. You may limit individual access to each application and may further limit access to each function within each application. System Logs provide an audit trail of all user activity within your NextGen SCP platform. Log types include: Communication Activity, Recording Access, System Access, Searches, Webpage Visits, and Data Change. This design delivers investigative recordings with digital clarity and provides easy remote monitoring from any secure web browser with internet access.

Securus Next Gen SCP features put you at the investigative intersection of Inmate management and communications management.

- 24x7x365 system monitoring
- Redundant backups for disaster recovery
- Securus manages 100% of maintenance and repair
- Regular rollouts of system updates at no additional charge
- System with single point of access inside or outside agency walls
- Automatic display of details
- Access anytime from anywhere

**e. A data analysis program will be provided to assist staff in reviewing inmate communications.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Word Alert™ is a powerful speech-to-text transcription and keyword search tool for corrections agency investigators. It automatically transcribes all telephone calls and Securus Video Connect (SVC) video sessions to text. Investigators can search the transcripts and Securus Text Connect (STC) text messages for words and phrases either interactively or by setting up automated, continuous scans that send them alerts when matches occur.

**Save time and get targeted leads:** Word Alert helps investigators quickly identify the communications most likely to have investigative value:

- Search for words and phrases interactively or by setting up automated, continuous scans with email or SMS notifications when matches occur
- Skim a transcript or text message conversation or jump to matching search terms rather than listening to the whole call or session
- Get an English translation of a non-English transcript
- Uncover individuals who are talking about topics of investigative interest—Intelligent analytics reveal topics now being talked about in the facility more than in the past, uncovering problems before investigators know to look for them.

Word Alert is a Securus solution and Securus manages the solution roadmap. It is integrated with the Securus NextGen Secure Communications Platform. No additional hardware is required. The interface for investigators is browser-based and runs on Windows.

### Word Alert Advantages

Word Alert provides these advantages for the agency and its investigators:

- Word Alert lets investigators search three types of communications for words and phrases of interest: telephone calls, SVC sessions, and STC text messages.
- A transcript of each telephone call and video session is available in minutes in its original language. \*
- An English translation can be requested and displayed in seconds in line with the original language text. \*
- Investigators can view a transcript alone or aligned with the audio or video player while the call or session plays. Search term matches are highlighted in the transcript. A button click jumps to the next or previous match in the transcript, moving the player automatically as well.
- Transcripts, text messages, and their translations can be saved to PDF files.
- Investigators can manage an editable dictionary of word and phrase search terms, in any language, and create categories of search terms.
- Interactive, ad hoc searches let investigators find words and phrases in past calls and sessions.
- Automated scans constantly search new calls and sessions for target words and phrases and send alerts to investigators when matches occur.

- Alert notifications can be sent to email addresses and SMS text phone numbers.
- Snippets of matches in transcripts appear when the investigator's mouse hovers over a list of calls, video sessions, and text messages. Mouse clicks jump to those locations in the player and transcript.
- Integrated audio and video players can control playback speed and volume.
- Search results can be exported to downloadable reports.
- Analytics include search term category frequency graphs and totals.
- Word Alert's intelligent, behind-the-scenes analysis uncovers trending topics of conversation on calls and sessions in the facility. This can reveal illicit activity before investigators realize it exists.
- Users' call and video session playback events are logged in the NextGen SCP system, giving agencies information for auditing.

\* The supported languages for transcription, and for translation to English, are Bengali, English, French, Italian, Korean, Mandarin Chinese, Polish, Portuguese, Russian, Spanish, and Vietnamese.

### Word Alert Capabilities

Word Alert capabilities include the following features:

- Simultaneous search of multiple types of communications
- Automatic speech-to-text telephone call and SVC video session transcription
- Rapid translation to English
- Transcript aligned with the audio and video player
- Dictionary of search terms
- Interactive searches of past calls, video sessions, and text messages
- Automated searches of new calls, video sessions, and text messages with user alerts
- Search results with snippets and highlighted matches
- Alert notifications to email addresses and SMS text phone numbers
- Integrated audio and video players
- Export transcript or text message conversation to PDF
- Call and video session playback logging

- Reports
- Analytics

## Simultaneous Search of Multiple Types of Communications

Simultaneously search telephone calls, SVC sessions, and STC text messages for words and phrases of interest. Investigators can also narrow their searches to one or two of those communication types.

## Automatic Speech-to-Text Telephone Call and SVC Video Session Transcription

Telephone calls and SVC video sessions are automatically transcribed to text within minutes after they end. There is no need to select any for transcription. Each text transcript is in the language the Inmate used when starting the call or session. Transcripts are stored in accordance with the agency's call and video session retention policies.

## Rapid Translation to English

The investigator can request an English translation of a non-English transcript with just a button click. The translation appears in seconds with each line under the original language line in the transcript. The English translation is stored with the original transcript for future reference.

## Transcript Aligned with the Audio and Video Player

A transcript can be viewed alone or aligned with Word Alert's audio or video player. Any search term matches are highlighted in the transcript. The investigator can jump to a section of interest in either the player or transcript and the two will move in tandem to that section. In the transcript they can jump from any search match to the next or previous match, and the player will move to that location.

## Dictionary of Search Terms

Word Alert has an editable dictionary of words and phrases that can be used as search terms. Investigators can add terms in any language and create categories of terms. Individual terms, or entire categories, can be used in searches.

## Interactive Searches of Past Calls, Video Sessions, and Text Messages

Word Alert makes it easy to do one-time, interactive searches of past calls, video sessions, and text messages using a date range and words, phrases, and categories of terms in any language. The search can be narrowed by Inmate name or ID and communication type, i.e., telephone calls, video sessions, and/or text messages. Results are displayed as a list of calls, sessions,

and text/or text messages, each with clickable icons to show the transcript alone or with the player.

### **Automated Searches of New Calls, Video Sessions, and Text Messages with User Alerts**

Word Alert lets investigators set up automated scans that continuously monitor new text messages and new call and video session transcripts as they come into the system. An alert is sent each time a search term match occurs in a call or session. The investigator configures an automated scan with search terms in any language and optionally with an Inmate's name or ID, as well as the communication type. They can also include an end date if they choose. An alert is sent to the dashboard each time a search term match occurs in a call or session. The investigator can add email addresses and SMS text message phone numbers to receive alert notifications as well.

At any time, the investigator can see the total number of alerts triggered so far by the scan. They can review the calls, sessions, and text messages that triggered the alerts and can also stop the scan at any time interactively. They can modify the alerts' lists of email and text message notification recipients.

### **Search Results with Snippets and Highlighted Matches**

Calls, video sessions, and text messages with matching search terms are each listed with their communication record information: name of the Inmate, dialed telephone number, communication start date and time, and communication duration. Each record also shows a player icon and a transcript icon. Hovering over the transcript icon brings up one or more snippets from the transcript. The snippets show the search term matches in context. The investigator can decide whether to bypass that communication or investigate it further. They can click on the transcript icon to open the full transcript, or the player icon to see the transcript with the player. The matching search terms are highlighted in the transcript or text message.

### **Alert Notifications to Email Addresses and SMS Text Phone Numbers**

Alerts can be configured to send email and/or SMS text message notifications. The investigator can set up the notifications when they create the alert or at any time afterwards. They can set the frequency of the notifications, modify (add, edit, delete) the email and text message recipients, and unsubscribe from notifications for a particular alert or all email and/or text message alerts.

### **Integrated Audio and Video Players**

The integrated audio and video players have user controls to regulate playback speed and volume. The audio player also allows the investigator to mute either side of the communication independently. In both players, the transcript and

player are aligned when they are displayed together. The investigator can play any portion of the call or session and read its transcript as they listen. Changing the location in either the player or the transcript changes it in both simultaneously.

### Export Transcript of Text Message Conversation to PDF

A transcript can be exported and saved to a PDF file. Any in-line English translation in the transcript is included as well. The text is formatted exactly as it is on the screen and includes timestamps.

### Call and Video Session Playback Logging

Whenever a Word Alert user plays part or all of an ITS call or SVC video session, that activity is logged in the NextGen SCP system logs. This provides auditing information for the agency.

### Reports

The results of an interactive or automated search can be exported to a report and then downloaded. The report lists calls, video sessions, and text messages that had matches, with communication record information for each one.

### Analytics

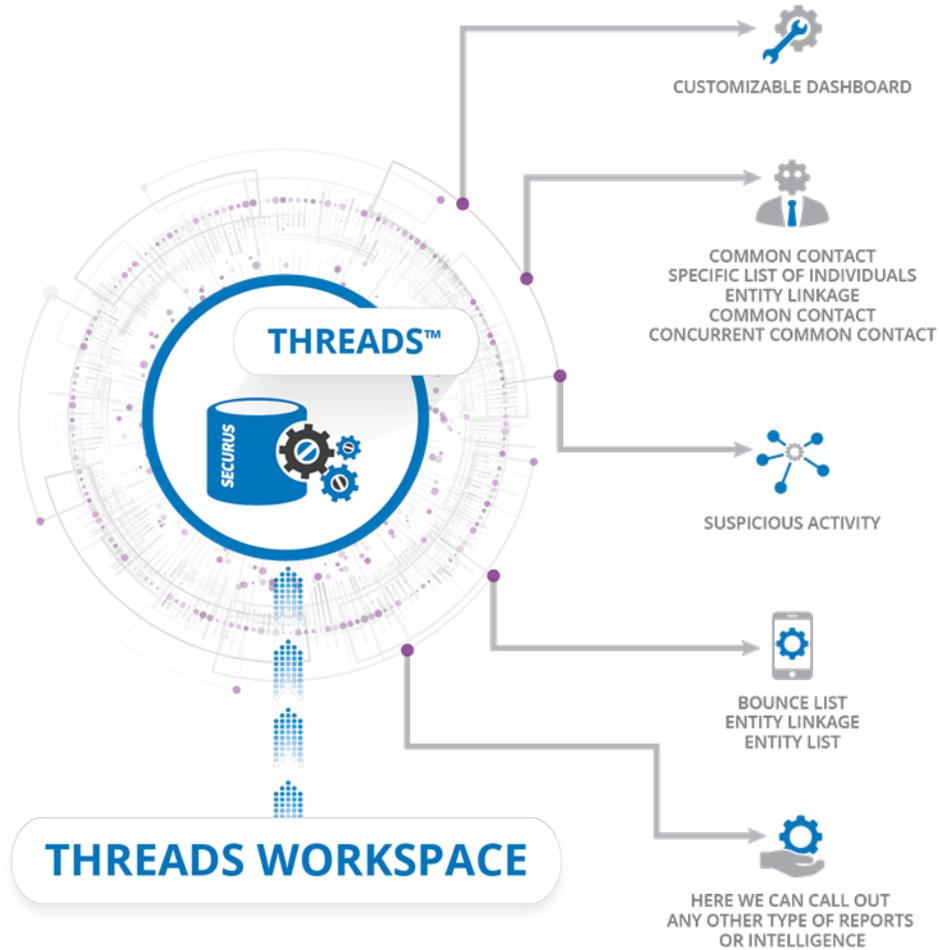
Intelligent analytics reveal what people in the facility are talking about on telephone calls, video sessions, and text messages without investigators having to do searches. In Analytics, the Keyword Categories screen shows how many times, and on which calendar days, words in each of the dictionary's categories occurred. The Top Keyword Trends screen shows additional words that Word Alert discovered on its own that are occurring in calls and sessions more often now than in the recent past. This trend information can uncover problems in the facility before investigators suspect they exist.

## THREADS™ Analytic Data Platform—Overview

Securus understands that during an investigation, the law enforcement community is inundated with tasks and gathering intelligence. Identifying relevant data can be a challenge at times when new data are identified. This results from numerous different sources, formats, and potential leads that require identification. **Through Securus' data analytics platform—THREADS™—facility data is automatically ingested the moment THREADS is enabled.** Additional external data sources can be imported and analyzed to build an investigation. **All of this takes place without purchasing any additional equipment, and can be managed remotely at any time through an assigned**

**web-based portal.** This means that Sedgwick County can access data remotely from any location that provides internet access.

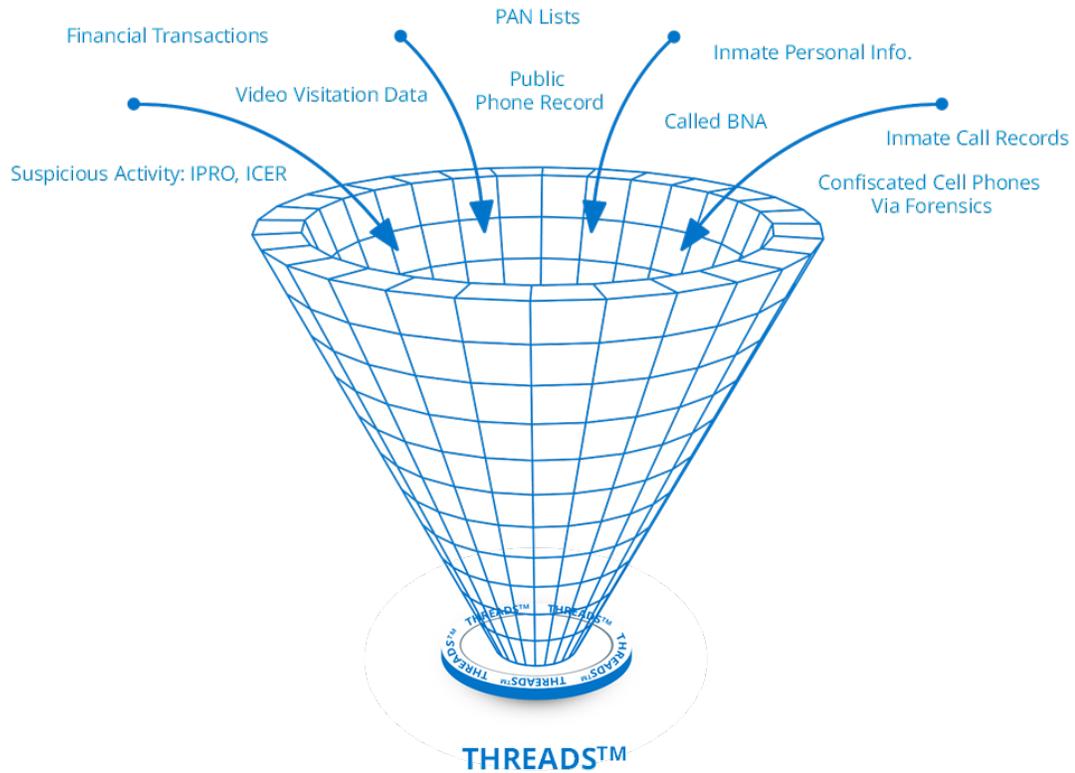
### THREADS Brings Big Data Capability to the Corrections Industry



### THREADS Applies Big Data Search Algorithms to Investigative Support

THREADS brings the power of Big Data Analytics to the investigative capabilities of correctional facilities, thereby reducing demands on Investigative personnel, while increasing their ability to identify potential criminal behavior. THREADS gathers and analyzes facility data, identifying actionable data that can be used as the basis of targeted criminal investigations.

## Data Pulled from Multiple Databases



THREADS automatically imports information from NextGen SCP's telecommunications database, Inmate information from JMS, and financial data. Multiple sources of data and databases are combined into the THREADS' analytic framework to reduce the time required for investigators to find suspicious patterns. Such patterns may be an indication of planning or commissioning crimes.

### Widely Used Investigative Telecommunications Platform

THREADS is the most widely used investigative telecommunications platform in the industry today, with more than 1.5 million Inmates served, multiple petabytes of aggregated intelligence data, and more than 2 million phone calls processed per day. THREADS' powerful data analytics engine analyzes multiple types of facility data, such as Inmate communication records, public phone records, billing name and address, data from confiscated cell phones, financial data, and more to automatically generate focused leads for investigators. THREADS' robust and accurate analytics engine is intuitive and easy to use, making it the ideal tool for any investigative officer operating within a correctional institution.

## THREADS Was Developed Specifically for the Corrections Industry

Unlike other investigational software, which requires users to manually upload facility data, THREADS automatically consumes facility data on a nightly basis and does not require any equipment to reside on site. **The unique algorithms within THREADS were designed in conjunction with high-profile investigators, bringing more than 50 years of combined experience in communications, data, and training.** What can take an entire day with multiple officers working eight-hour shifts now takes just moments.

### Primary Benefits of THREADS to the Prison Community

The primary benefits of THREADS to the prison community include:

- Visually based linkage reports that make the identification of communication patterns and the identification of Inmate activities and communications quick and easy to understand.
- Significant reductions in the amount of investigative time required to produce documented and actionable results.
- Community Data Sharing allows facilities to run reports on a much larger data set to expand their investigative reach.
- Customizable facility dashboard with configurable display-based facility metrics.
- Discovery and disruption of Inmate-based criminal activities.

### Importing Information

THREADS will automatically import the **following types of corrections information:**

- Inmate call records
- Inmate personal information, such as name, account number, PIN, DOB, SSN, and more
- PAN lists
- Called party billing name and address information
- Video visitation data
- Suspicious activity, through IPRO and ICER for example
- Financial transaction metrics

THREADS can also import **information from external data sources, such as:**

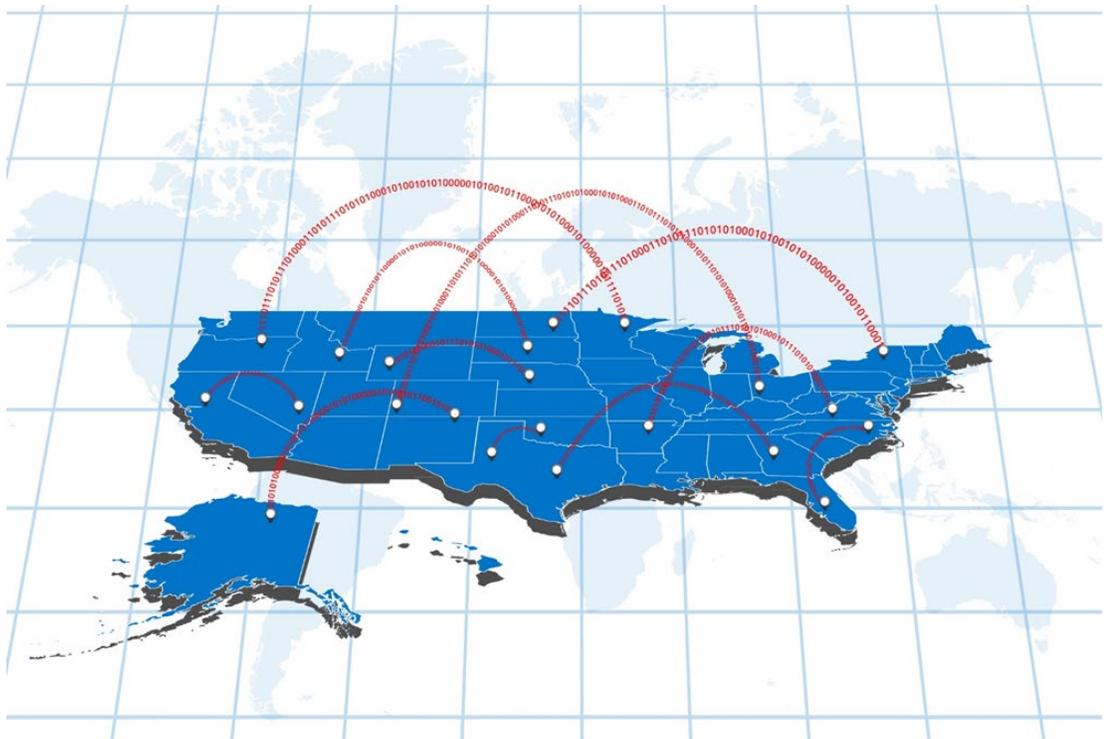
- Confiscated cell phones—calls, text messages, emails, videos, contacts, etc.
- Public phone records, as legally allowed
- Events and places of interest
- Mail
- LexisNexis

## THREADS Communities

THREADS further separates itself from other Inmate telephone service providers by providing a national community database where facilities can choose to share their data to expand and identify more investigative opportunities and leads. Facilities can choose to share data with other local, regional, or national agencies depending on their investigative needs.

Through this community of data sharing, THREADS users can leverage the resources of other agencies to understand the breadth of their investigations and, therefore, close cases faster. By joining the THREADS community, users can run reports, uncover data correlations, and gather contact information unlike any other data analytics solution.

### THREADS Communities Share Data Between Multiple Jurisdictions

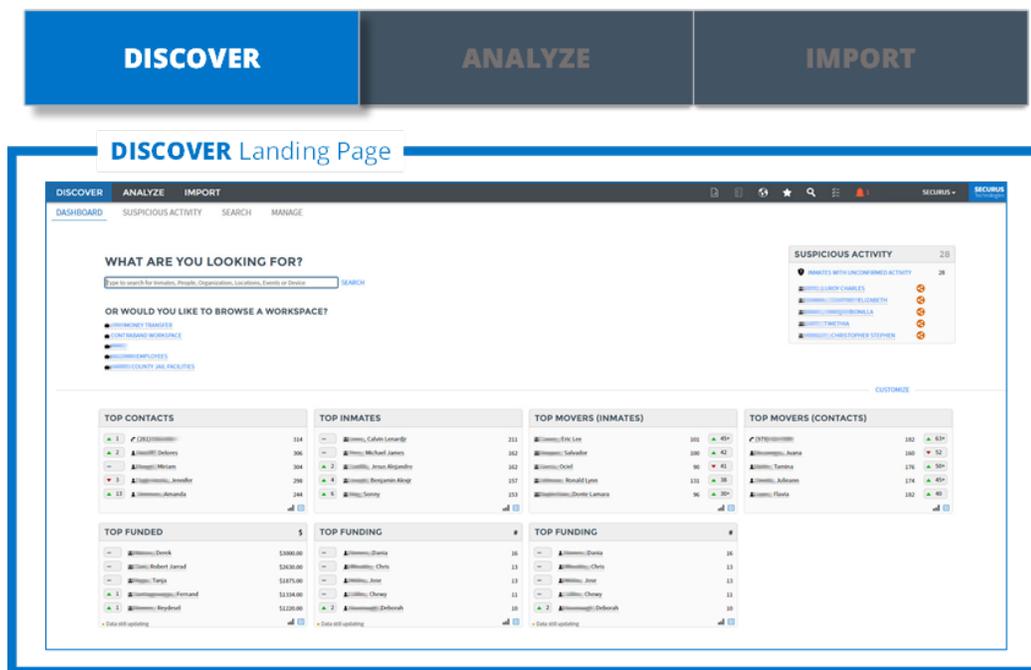


## Discover / Analyze / Import

To make it easy and intuitive, THREADS is divided into three sections—**Discover**, **Analyze**, and **Import**. Each of three major activities are contained in each section, making it easy to identify which activity the investigator wants to initiate. Details of what items are contained in each section are provided below:

- **Discover**—Define, run, and view reports on information gathered and categorized by THREADS.
- **Analyze**—Define the types of analysis to be performed and runs the automated analysis built in THREADS.
- **Import**—Define sources of data to be automatically imported. This includes data from external sources, such as subpoenaed phone records; confiscated cell phone forensics; data extracted from JMS, RMS, and other systems and data.

THREADS *Discover* Landing Page (Dashboard)



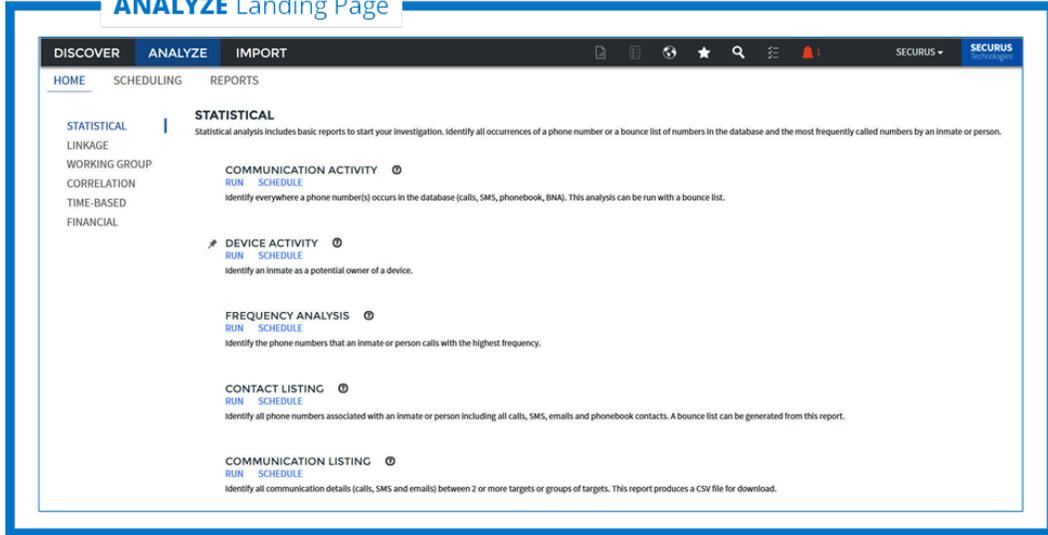
### Widgets

The **Discover** landing page shows customizable widgets allowing the investigator to set up information in a way that is most convenient to their investigative needs. These widgets default to the following categories: Suspicious Activities, Tasks, Top Inmates, Top Contacts, and Recent Records.

## Threads *Analyze* Landing Page



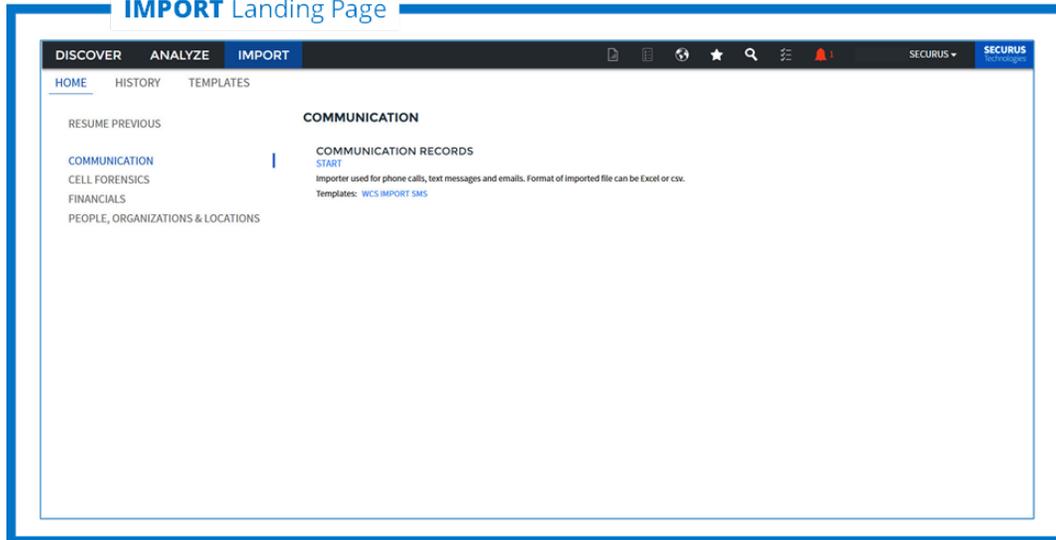
### ANALYZE Landing Page



## THREADS *Import* Landing Page



### IMPORT Landing Page

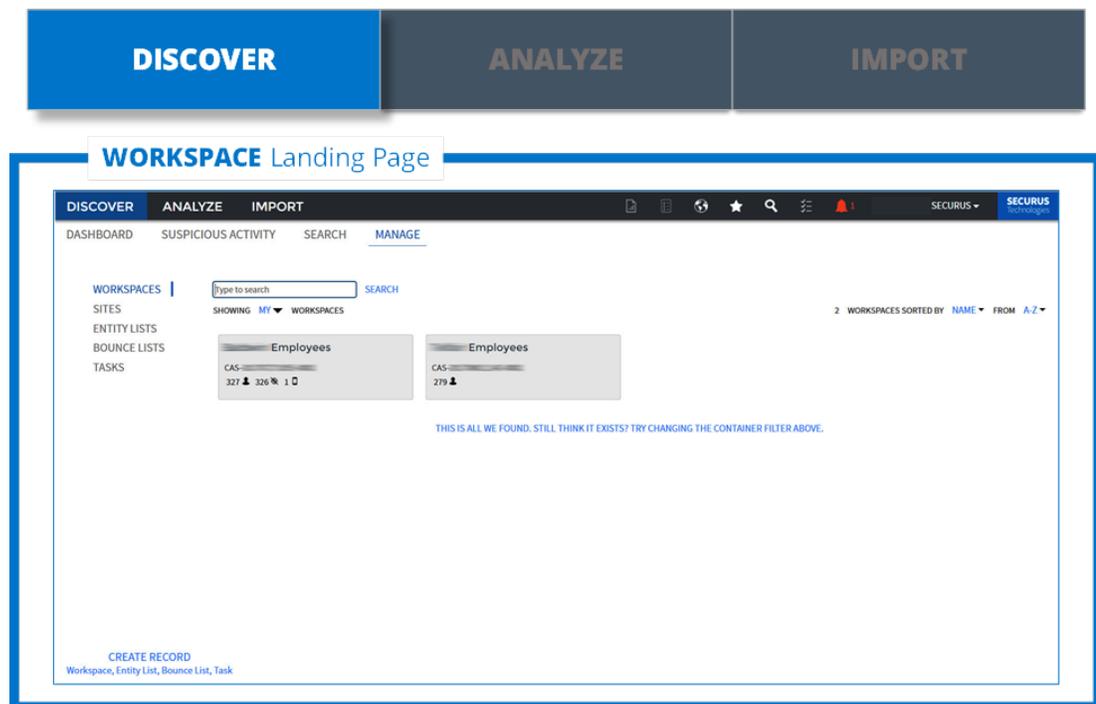


## Frequently Used Features

### Workspaces

Within THREADS, Securus provides online workspaces where investigative cases can be built. These workspaces allow users to compile data and build an investigation. Pictures, locations, devices, organizations, and known associates can be inserted and attached within the workspaces to organize in-progress investigations while investigators add additional data points. Investigators can update the permissions for each workspace to allow only the active investigator, only Sedgwick County facilities, or your full shared community to have access to individual workspaces. Through these settings, users filter editing privileges for those assigned with viewing access.

#### THREADS Workspace



### Graphic and Textual Information

All information is presented graphically as well as textually. Timeline charts and graphical analysis make it easy to reveal periods of high-intensity calling and other calling patterns on a graphical and interactive timeline.



- Working Group
- Correlation
- Time-Based
- Financial

These report types are described in the following pages.

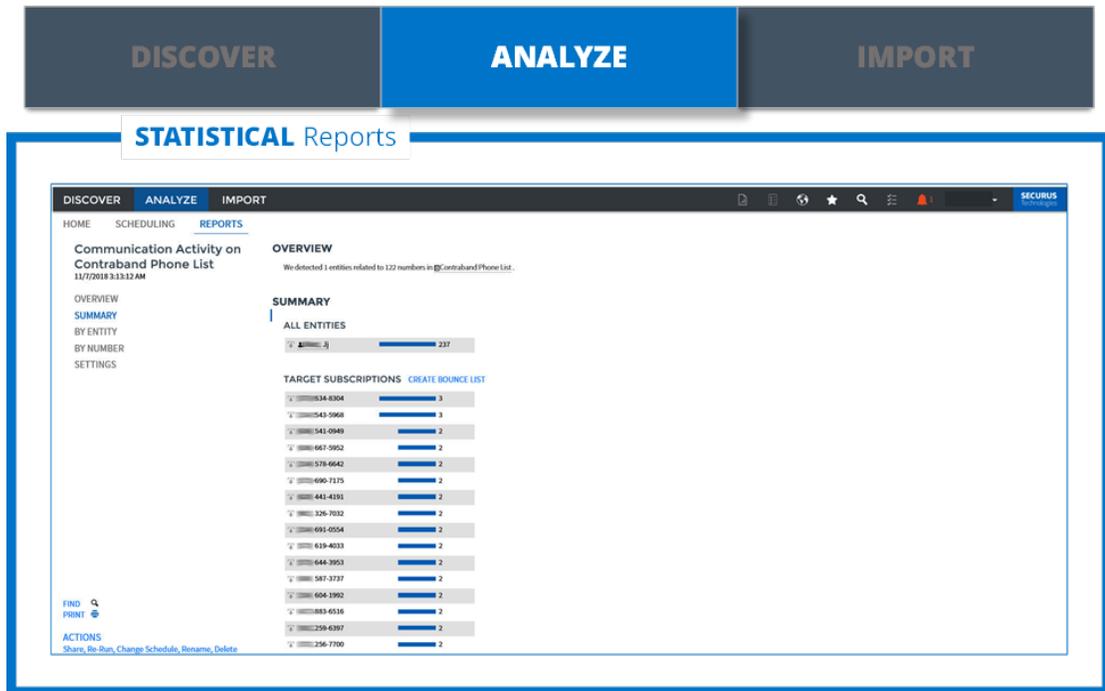
### Statistical Reports

Statistical analysis includes basic reports to start your investigation. This includes all occurrences of a phone number or a bounce list of numbers in the database and the most frequently called numbers by an Inmate or person.

Investigators can:

- Identify everywhere a phone number occurs in the database, such as calls, SMS, phonebook, and BNA. This analysis can be run with a bounce list.
- Identify an Inmate as a potential owner of a device.
- Identify the phone numbers that an Inmate or person calls with the highest frequency.
- Identify all phone numbers associated with an Inmate or person including all calls, SMS, emails, and phonebook contacts. A bounce list can be generated from this report.
- Identify all communication details (calls, SMS, and emails) between two or more targets or groups of targets. This report produces a CSV file for download.

## Sample Statistical Reports



### Linkage Reports

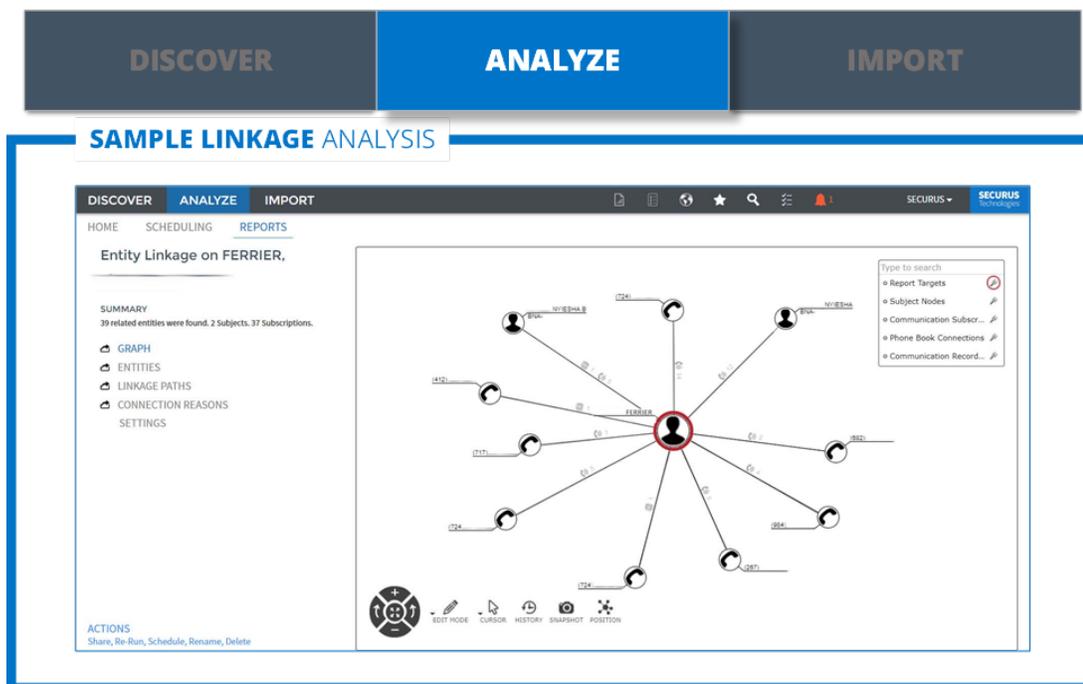
Linkage analysis shows how Inmates and people are related. All the reports in this section generate graphical results that let you explore the relationships between your targets. This visual reporting tool is a quick way to understand who Inmates are talking to and how the calls are related to other known numbers or Inmates.

Users can generate a linkage chart that identifies the following information based on user-selected connection types, such as calls, financials, visitation, etc.:

- A target(s) relationships
- Connections between two selected targets or two sets of targets
- Connections between two or more targets

In addition, users can generate a linkage chart that identifies direct relationships between selected targets based solely on phone calls.

## Sample Linkage Analysis



### Working Group / Inner Circle Reports

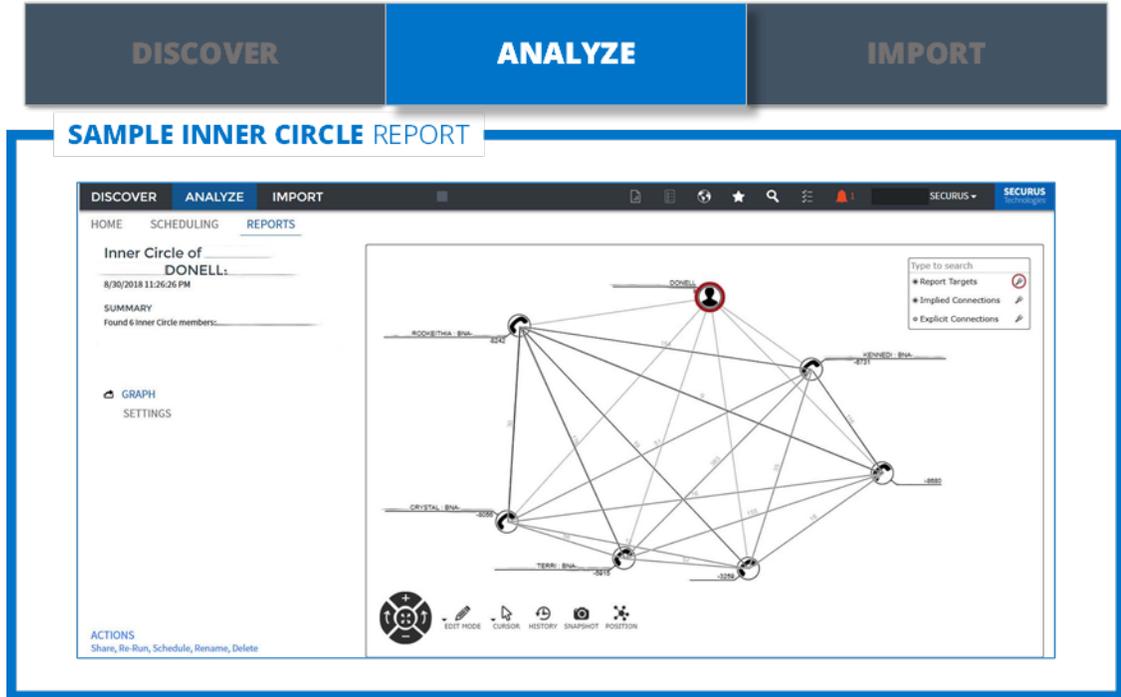
Working Group analysis uses a person's communication behavior and calling patterns to identify phone numbers and people of interest. One of the key techniques used is temporal analysis, which links people based on time between calls. The closer the time between calls, the more likely those calls are related. By leveraging working group reports, facilities can identify gang and other organized activity. Knowledge of organized groups and gangs can aid staff in monitoring member activity or take preventive measures against illicit activities.

Investigators can:

- Identify a target's "working group" or inner-circle based on their communication patterns. This report is a graphical linkage chart.
- Display a target's inner circle changes over a predetermined time.
- Show communication sequences where a target calls two or more numbers in a pattern.
- Identify communication patterns—such as two or more of the same sequence—and when they occurred.
- Find a target's chain of calls. A chain is a series of calls triggered by the previous call in the chain. This report requires imported phone calls from outside the facility.

- Identify the most-likely boss in an organization based on chain analysis. This report requires imported phone calls from outside of the facility.

### Sample Inner Circle Report



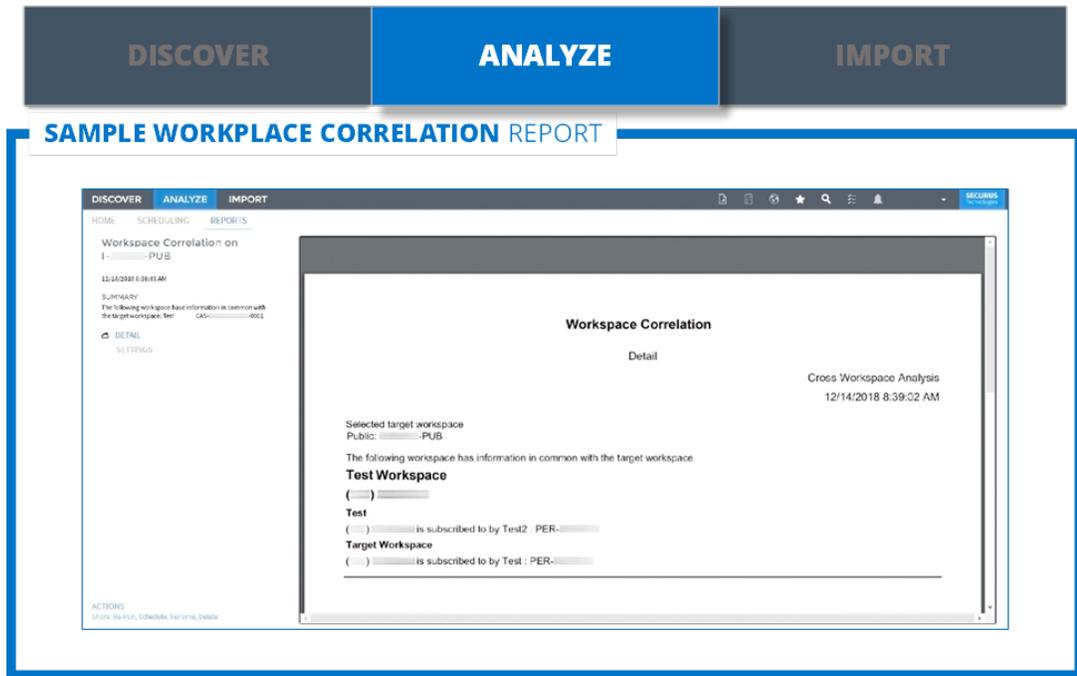
### Correlation Reports

Correlation analysis identifies common contacts and phone numbers between Inmates, persons, and workspaces. Through correlation reporting, investigators can identify common contacts between Inmates as well as fraternization between Inmates and facility staff.

Investigators can:

- Find any common communications between Inmates, persons, or groups of targets.
- Identify potential three-way calls between Inmates.
- Discover common phone numbers between two workspaces.

## Sample Workplace Correlation Report



### Time-Based / Hole Detection Reports

Time-based analysis provides reports based on the timing and frequency of an Inmate's or other person's communications. The investigator can find out when communication is frequently taking place, then identify periods of time where communication is not taking place. These gaps in communication can indicate behavioral changes as well as cell phone usage.

Investigators can:

- Identify holes or gaps in an Inmate's or person's communication activity.
- Display a set of phone numbers that a person called where communications stop with one phone number and communications start with a different phone number within a proximity of time. This might indicate a change of phone number or an organizational shift.
- Identify if two or more phones are being used at overlapping times. If there is a significant time overlap, it could indicate that the phones are being used by different people.
- Generate a graphical timeline of any activity—such as communication, association, financial transactions, etc.—that includes a date and time.

## Sample Hole Detection Report

DISCOVER
ANALYZE
IMPORT

DISCOVER
ANALYZE
IMPORT

Hole Detection on

MARCUS

11/8/2018 3:01:30 PM

Department Of Criminal Justice,

Hole Detection

Start Time	End Time	Duration
11/13/2017 4:31:01 PM	11/18/2017 5:07:59 PM	5 days 36 minutes 58 seconds
11/26/2017 2:57:31 AM	11/28/2017 12:19:24 AM	1 day 21 hours 21 minutes 53 seconds
11/28/2017 1:24:22 PM	11/29/2017 2:01:12 PM	1 day 36 minutes 50 seconds
11/30/2017 12:05:01 AM	12/02/2017 12:49:54 AM	2 days 44 minutes 53 seconds
12/3/2017 9:24:01 PM	12/4/2017 11:31:40 PM	1 day 2 hours 7 minutes 39 seconds
12/5/2017 4:44:42 PM	12/8/2017 12:46:15 AM	2 days 8 hours 1 minute 33 seconds
12/8/2017 1:21:37 AM	12/9/2017 5:19:29 PM	1 day 15 hours 57 minutes 52 seconds
12/9/2017 5:19:29 PM	12/11/2017 1:16:12 AM	1 day 7 hours 56 minutes 43 seconds
12/11/2017 11:44:26 PM	12/13/2017 1:25:25 PM	1 day 13 hours 40 minutes 59 seconds
12/14/2017 4:24:45 PM	12/16/2017 4:27:08 PM	2 days 2 minutes 23 seconds
12/17/2017 2:24:40 PM	12/19/2017 2:23:46 AM	1 day 11 hours 59 minutes 4 seconds
12/19/2017 3:58:08 PM	12/23/2017 2:14:47 AM	3 days 10 hours 16 minutes 39 seconds
12/24/2017 1:50:00 AM	12/25/2017 7:21:08 PM	1 day 17 hours 31 minutes 8 seconds
12/26/2017 1:28:08 AM	12/27/2017 10:03:28 PM	1 day 20 hours 35 minutes 20 seconds
12/28/2017 3:47:54 AM	12/29/2017 4:17:46 PM	1 day 12 hours 29 minutes 52 seconds
12/29/2017 4:17:46 PM	12/31/2017 1:26:47 AM	1 day 9 hours 9 minutes 1 second
1/1/2018 3:07:30 AM	1/2/2018 3:13:34 AM	1 day 6 minutes 4 seconds

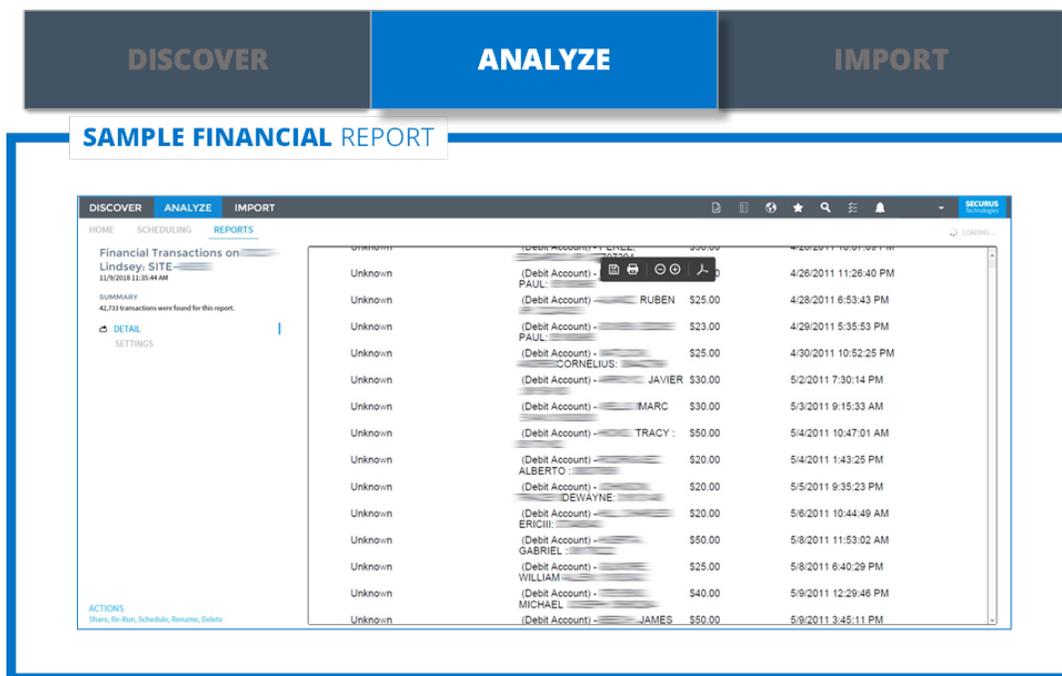
## Financial Reports

Financial analysis identifies correlations between Inmates and people based on the funding of an Inmate's accounts.

Investigators can:

- Identify Inmate financial accounts with multiple funding sources.
- Identify and list financial transactions of interest for a set of targets.

## Sample Financial Report



### Efficient Automated Reports

When key information is gathered, investigators must determine where all of that data will go and then take part in the time-consuming method of analysis. However, THREADS takes it one step further by allowing facilities to set up automated reports. Reports can be scheduled to take place daily, weekly, or monthly. Through this automated reporting process, users receive notifications regarding the data they use at the timeframes they select.

### Managed Data Analytics

For facilities interested in using THREADS but requiring additional investigative resources, Securus offers Guarded Exchange to provide this service. Guarded Exchange is a fully owned Securus subsidiary, managed by current and former law enforcement and corrections personnel. With more than 20 years of experience, Guarded Exchange has the resources to run THREADS reporting and analytics, and provide actionable intelligence to Sedgwick County facility members. Guarded Exchange is here to serve Sedgwick County by importing and filtering data to provide the investigative leads that Sedgwick County needs.

### Conclusion

THREADS offers the flexibility for investigators to reference and cross-reference internal and external data on demand and all within an easy-to-use platform.

From high-level facility metrics, to the import of contraband phone data, THREADS offers the most comprehensive investigative software solution in the market with a robust data analytics and reporting toolset **specifically developed for the corrections industry. THREADS is 100% owned and maintained by Securus Technologies** and provides updates and enhancements through regularly scheduled upgrades and deployments. THREADS continues to invest in research and development to lead the market with the new features and functions necessary to stay current with the growing needs within your facility.

- i. **Provide a detailed explanation of the data analysis program including search functions, available reports, and management tools.**

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Securus NextGen SCP™ gives investigators access to tools for their investigations** and lots of options for efficient searches: search for calls and video sessions using criteria such as called/visiting party, calling phone, date, time, PIN, account, duration, and locations; search across a single site or group of sites based on the user's security authorization; or search based on call attempts or filter for completed calls/video sessions. Search results provide detailed information about the call/video and indicate the presence of a recording.

NextGen SCP™ includes a **powerful player that investigators use to listen to or watch recordings**, within the limits of their security access. The player includes easy-to-use search capabilities, and features such as pause and fast-forward. For calls, a visual waveform helps investigators bypass areas of limited talk time and quickly identify particular events. You may also mute one of the speakers to focus on the other.

**Chain of evidence safeguards prevent access to the original recording** to eliminate any chance of intentional or accidental manipulation or deletion. When listening to a recording, the audio is "streamed" to the user's computer further safeguarding the original recording.

Communication events less than one year old can be retrieved within the requested timeframe. Communication recordings that are marked "store for life of contract," could take slightly longer to retrieve because of the required data mining.

#### **Note-Taking and Tracking in NextGen SCP**

NextGen SCP allows authorized users to add notes and tracking numbers to communication detail records associated with recordings. This feature is

accessed via the notepad icon in the communication detail record. To any communication, you can add notes such as a tracking number, gang affiliation, and duration into the call. The note author chooses whether to share the note with other users or mark the note as private to their investigation. From the Notes tab on the communication detail record, users may view previous public notes associated with the communication.

## Adding a Note to a Communication Detail Record

The screenshot displays the 'COMMUNICATION SEARCH' interface. At the top, there is a navigation bar with 'SECURUS Technologies' and various menu items like 'Dashboard', 'Monitor', 'Explore', 'Investigate', 'Manage', and 'Admin'. Below this is a search bar with '2 Search Types' and a date range filter for 'Communication Date Range (PT)'. The search results show two entries:

Type	Inmate Name (ID)	Other Party	Start Date/Time (PT)	Duration	Notes	Flag
Video	Nizon, Beter (MRK0003)	JOE HIGGS	09-09-2018 8:00:00 AM	00:00	[Note icon]	
Phone	Carver, Sam (0080)	1 (817) 896-XXXX	09-07-2018 12:06:17 PM	08:56	[Note icon]	[Flag icon]

Annotations on the screenshot include:

- A blue box with the text 'Select the communication record.' and a red arrow pointing to the first search result.
- A green 'Add Note' button with a notepad icon.
- A blue box with the text 'Click "Add Note" to add a note to the selected' and a red arrow pointing to the 'Add Note' button.

Sedgwick County can use the Advanced Search function to search for notes based on the CDR tracker number, note type (no notes, my private notes, or shared notes), or keywords—such as a gang affiliation—within the CDR tracker notes. As with every report in the NextGen SCP user interface, the results are exportable to Excel, PDF, or CSV.

## Communication Reporting in NextGen SCP

Authorized Sedgwick County users can generate communication reports on all SVC events through the NextGen SCP™ user interface. Sedgwick County users can perform a dynamic search using the single input omnibox or an advanced search.

## Searching for SVC Events

SECURUS Technologies | Dashboard | Monitor | Explore | Investigate | Manage | Admin | NG SCP Demo

### COMMUNICATION SEARCH

Search: 2 Search Types | Search by any combination of inmate name, custody account numt | 08-30-2018 04:00 PM - 08-31-2018 11:59 PM | Search

Search by inmate name, custody account number, PIN, dialed number and/or terminal.

Search by popular tags: Public Private

- Fun Times One
- TWH
- Rob Widner
- DLM
- Cecilia Truong
- JGL082118
- Training
- JGLEAU82218
- KM\_TestCD

Function	Format	Instruction
OR	This That	To find items that might use one of several words, use a space between.
Wildcard	Th*	Add an asterisk as a placeholder for any unknown or wildcard terms.

Phone Number Formats

- (123) 456-7890
- 123-456-7890
- 1234567890
- 123 456 7890
- (123)456-7890

## Advanced Search for SVC Communication Records

SECURUS Technologies | Dashboard | Monitor | Explore | Investigate | Manage | Admin | NG SCP Demo

### ADVANCED SEARCH

Dynamic Search | Search

Communication Date Range (PT) Required: 08-30-2018 04:01 PM - 08-31-2018 11:59 PM

Tag Name: | CDR ID: | CDR Tracker #: | CDR Note Type: |

Inmate ID: | Inmate PIN: | Inmate Site/Terminal Group/Terminal: | CDR Tracker Notes: |

Inmate First Name: | Inmate Last Name: |  All |  EPMO Next Gen Demo |  Marketing Next Gen Demo | Alt ID: | Alt Group: |

Communication Type: | Communication Status: | Private | YES NO BOTH

Calls

Country Code: | Phone #: | Prepaid Account #: | Destination Zone: | Watched: YES NO BOTH

Call Termination Category: | Inmate Agency Type: | Wireless: YES NO BOTH

Continuous Voice Verification (CV): YES NO BOTH

General Calls

Call Type: | Blocked Reason: |

3-Way: YES NO BOTH | Voicemail Accessed: YES NO BOTH

Remote Call Forwarding (RCF): YES NO BOTH | AIS Voicemail: YES NO BOTH

Live Connect: YES NO BOTH

NextGen SCP presents the search results in such a way that further action can be taken from this same page to further refine search results, download recordings or data, or export report results without navigating away from the search results page. The left side of the page offers filtering based on the results and shows only the filter options that are present in the results.

Clicking on the event in the results pane opens the communication event detail pane on the right side of the page. This pane provides additional detailed information about the event and allows the user to download the session report, extend the recording expiration date, download the video session, or play the session recording without downloading it to the user's computer.

### Securus Video Connect<sup>SM</sup> Communication Detail Report

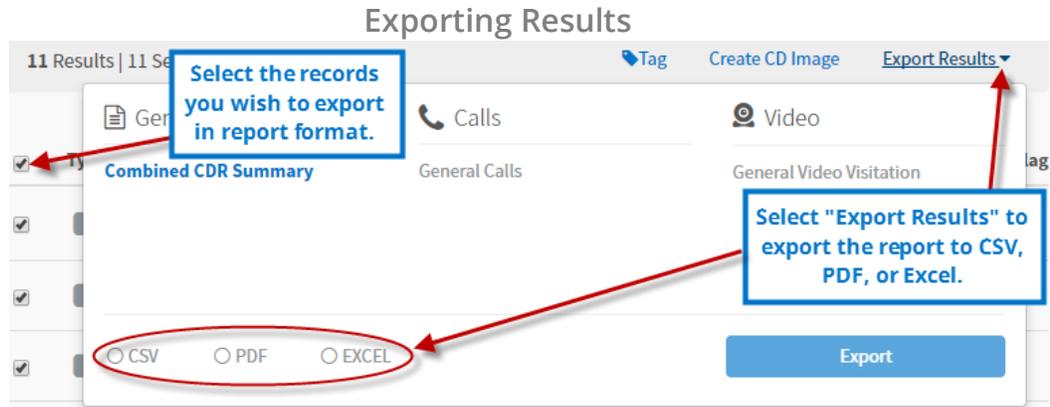
The screenshot displays the 'ADVANCED SEARCH' interface with the following components:

- Navigation Bar:** Includes 'SECURUS Technologies', 'Dashboard', 'Monitor', 'Explore', 'Investigate', 'Manage', 'Admin', and 'Marketing Next Gen Demo Site'.
- Search Criteria:** Shows 'Communication Date Range: 08-01-2018 11:59 AM ~ 08-22-2018 11:59 AM', 'Inmate: 1', 'Call: 0', and 'Video Visitation: 0'. Buttons for 'Edit Search' and 'New Search' are present.
- Filtering Panel (Left):** Labeled 'Refine by' and 'Expand All'. It lists various filters such as Agency Type, Communication Status, Tags, Inmate Terminal Group, Inmate Terminal, Visitor Terminal Group, Visitor Terminal, Termination Category, Visit Type, and Visitor Type. An 'Apply Filters' button is at the bottom.
- Search Results (Center):** Shows '45 Results'. A table lists communication events with columns for Type, Inmate Name (ID), Other Party, PT, Duration, Notes, and Flag. The first row is for 'Carter, Sam (0080)' on 08-22-2018 at 9:45:28 AM with a duration of 39:33.
- Details Panel (Right):** Titled 'Details', 'Notes', and 'History'. It contains a 'Session Report' section with buttons for 'Download Session Report', 'Extend Expiration', and 'Download Video Session'. Below this is a 'Session Info' section with fields for Inmate ID, PIN, Visit with, Start Time, End Time, Scheduled Start, and Scheduled Duration.

Callouts in the image provide the following instructions:

- 'Further refine your search results by filtering available criteria.' (points to the filtering panel)
- 'Click the event result to see video communication record details.' (points to a row in the results table)
- 'Options to download a report, extend the expiration date, or download the video session.' (points to the buttons in the details panel)
- 'Event details appear on the side panel.' (points to the details panel)

*Communication detail results can be exported to CSV, PDF, or Excel.*



**f. On site technician to address maintenance concerns across all platforms.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus will continue to provide Sedgwick County with an on-site technician to address any maintenance concerns. Damien Ashley and Field Tech Matt Journey, who you are already familiar with and who understand your operations, will continue to serve Sedgwick County.

**g. Vendor will supply an inmate broadcast system of capable of displaying information in the housing units in real time.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The Securus Services Application provides Sedgwick County with a streamlined communications tool to reach your population with real-time communications. Using the Officer Tablets, Sedgwick County authorized staff may send messages, notices, and bulletins to a single tablet, a group of tablets, or to all tablets. The Services App may also be used to send messages on Officer Tablets to one or more members of your team.

An FAQ on the Services App answers inmate frequently asked questions about Securus EVOTAB Tablets and Apps. In addition, an inmate may use the Services App to submit a Service Request to report any issues with their Securus EVOTAB Tablet. All communication is logged and tracked for security purposes.

- i. Must of capable of displaying messages or alerts created by staff. This can be accomplished using the kiosks in the pod or by using a standalone broadcast system.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Staff-created messages or alerts can be displayed using kiosks or inmate tablets.

Sedgwick County requires a turnkey inmate communication solution which shall include, without limitation, collect, pre- paid collect, paperless debit interface with the commissary provider, international collect calling, free calling to specific services, video visitation service including an option for free on-site video visitation, inmate tablets at a 1:1 ratio at the Annex Facility (approximately 180), mail scanning and digital delivery, and an electronic inmate request and grievance system. Vendor shall install and operate inmate phones, video visitation devices, tablets, grievance and request system, and all related equipment. Vendor shall, without cost to county, provide all wiring for the inmate telephones and video visitation devices, install the inmate telephones and visitation devices and the related hardware and software specifically identified herein, to enable inmates at the facilities to complete, without limitation, local, long distance and/or international collect, pre-paid collect, debit and free calls as well as visitation sessions from the facilities.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus is prepared to deliver a comprehensive turnkey inmate communication solution that meets all requirements outlined by Sedgwick County through the life of the contract. This includes the installation of all new equipment and the latest generation of the NextGen SCP™ inmate telecommunications system. Our solution will include, but is not limited to:

- Collect and pre-paid collect calling
- Paperless debit interface with the commissary provider
- International collect calling
- Free calling options to specific services
- Video visitation services, including an option for free on-site video visitation
- Inmate tablets provided at a 1:1 ratio for the Annex Facility (approximately 180 tablets)
- Mail scanning and digital delivery
- An electronic inmate request and grievance system

We will install and operate all inmate phones, video visitation devices, tablets, and related systems at no cost to the county. This includes providing all necessary wiring for the inmate telephones and video visitation devices, along with the installation of hardware and software specified in this proposal. Securus assigns fully qualified, factory-trained field technicians to inspect shipped equipment, and install and maintain NextGen SCP for the duration of the contract period. Our aim is to enable inmates to seamlessly complete local, long-distance, and international calls, as well as participate in visitation sessions from the facilities.

**Vendor shall supply details of Vendor’s proposed ITS which shall include, but not be limited to: system version (if Proposer uses multiple ITS versions and/or releases), system design (centralized vs. premise-based), technical specifications, software applications, hardware architecture and networking capabilities. Vendor shall also include a description, as well as visual aids, of the inmate phones, tablets, video visitation devices, inmate grievance system, TDD units and cart/portable sets proposed for installation at the Facilities.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Industry-leading technology with input from corrections and law enforcement partners:** The NextGen SCP (Version 24.3.0.) is an integrated software platform for managing, researching, monitoring, investigating, and exporting information through Securus products and services. Built from the ground up with input from corrections and law enforcement professionals, Securus NextGen SCP has the industry-leading technology, features, and functionality you need to manage communications and support investigations at your facilities. Securus’ Video Connect platform will undergo a major update in 2025. Please talk with your Account Manager for more details about this plan.

- Integrated interface to manage communications and investigations
- Reliable network and secure data storage with built-in redundancy

Securus NextGen SCP Key Features
<p>Refined User Interface</p> <ul style="list-style-type: none"> <li>• Easily maneuver with action-based navigation</li> <li>• Use Google-like single entry search fields</li> <li>• Get more information with less effort in a shorter amount of time</li> </ul>
<p>Custom Dashboard Configurations for Easy Data Viewing at Login</p> <ul style="list-style-type: none"> <li>• See summary overview of facility communications immediately</li> </ul>

<ul style="list-style-type: none"> <li>• Quick access to BNA and PAN frequency search functionality</li> <li>• Access upcoming video sessions</li> </ul>
<p>Improved Records Search Experience</p> <ul style="list-style-type: none"> <li>• Increase the speed from request to data reducing your investigative time</li> <li>• Get multi-product results with a single search</li> <li>• Integrated backend technologies analyze and store data efficiently for fast access</li> <li>• Run reports in the background while continuing to work and get notice when ready</li> </ul>
<p>Comprehensive Population Oversight</p> <ul style="list-style-type: none"> <li>• A convenient activity stream shows all past, present, and future communication events</li> <li>• Manage settings and suspensions for calls, video, and other products independently</li> </ul>
<p>Single Platform to Manage Calls, Video, and Visits</p> <ul style="list-style-type: none"> <li>• Use the Contact Profile page to view visitor information and manage visits</li> <li>• Set up facility and site level approvals custom-designed for your needs</li> <li>• Manage visit approvals flexibly at first visit only, every visit, or automatically</li> </ul>
<p>Security and Access Management Flexibility</p> <ul style="list-style-type: none"> <li>• Provide users with access and edit rights only to information needed to do their job</li> <li>• Easily craft custom task-based permissions for admin. and investigative teams</li> <li>• Protect your facility access with required strong passwords and regular updates</li> <li>• Provide facility affiliated personnel with access to video sessions</li> </ul>

**Data, security, and control over communications:** NextGen SCP gives you fast and efficient access to communication data, increased security, unparalleled control over Inmate communications, and real-time alerts. Your data gathering systems will work together and deliver key insights in one place. NextGen SCP is entirely web-based, so your authorized users may access the system at any time, from any location.

**Backed by high-performance data center:** The back-end equipment for NextGen SCP is housed in a carrier-class, commercial-grade data center built to the latest technology

standards. This includes all hardware and software, fraud controls, investigative features, user utilities, call/video processing, and communication event recording. The hardware and software components adapt to the changing needs of your facility's operations, and can monitor, record, and block/unblock communication, and generate reports in real time.

Premise equipment includes Adtran and Cisco routers and IADs (Integrated Access Devices) that convert VoIP to analog signals for the Securus systems. Securus-provided workstations are the latest generation Dell processors, with Dell flat screen monitors and HP inkjet printers. Netgear or Cisco switches connect workstations to the Securus network.

**Corrections-grade equipment to withstand harsh conditions:** The traditional telephones are shock-resistant correctional facility-grade equipment that are hearing aid-compatible and mounted to ADA standards, where applicable. The video session terminals are correctional facility-grade with tamper-proof steel enclosures, shatterproof touchscreens, a high-resolution video camera with integrated lighting, and heavy, molded plastic handset with an armor-reinforced cord for audio communication.

**Real-time administrative control over communications:** Securus NextGen SCP, as a single-point-access user interface, gives Sedgwick County complete control over your systems in a simple, reliable, secure environment. The system adapts to your facilities and operations, rather than requiring you to conform to the software. Authorized users can apply settings and configurations in real time to turn on a device/terminal, restrict a device/terminal, change a blocked number, administer approvals for call and video lists, and turn on/off features and applications.

## SECURUS NEXTGEN SECURE COMMUNICATIONS PLATFORM

### WELCOME

Welcome to the **SECURUS NextGen Secure Communications Platform (NextGen SCP)**. If you have a Secure Communications Platform account, login on the right.

To sign up for a SECURUS NextGen Secure Communications Platform account, please contact your Securus Account Manager or call Securus Technical Support at 1.866.558.2323.

### PLEASE LOGIN

USERNAME

PASSWORD

LOGIN

[Forgot your password?](#)



**Secure, any time/anywhere access:** To access the Securus NextGen SCP interface, your users will open a Chrome™ browser and launch the URL: <https://ngscp.securustech.net/login>. After entering a valid username and password, all integrated features are accessed with just the click of a mouse. Securus NextGen SCP™ is protected by SSL (secure socket layer) security, which uses the same security protocols that banks use for establishing a connection for customer online banking.

**Information at your fingertips:** The Securus NextGen SCP dashboard is a configurable landing page giving quick access to often-used functions and a proactive overview of your communication systems in user-specific widgets. The Announcement Panel is where Securus posts notices about system maintenance, feature enhancements, and training opportunities.

**Sedgwick County control over access rights:** Assign access rights to each user role to control access based on the facility's security clearance objectives. You may limit individual access to each application and may further limit access to each function within each application. System Logs provide an audit trail of all user activity within your NextGen SCP platform. Log types include: Communication Activity, Recording Access, System Access, Searches, Webpage Visits, and Data Change. This design delivers investigative recordings

with digital clarity and provides easy remote monitoring from any secure web browser with internet access.

Securus Next Gen SCP features put you at the investigative intersection of Inmate management and communications management.

- 24x7x365 system monitoring
- Redundant backups for disaster recovery
- Securus manages 100% of maintenance and repair
- Regular rollouts of system updates at no additional charge
- System with single point of access inside or outside agency walls
- Automatic display of details
- Access anytime from anywhere

Securus' inmate telephones are designed specifically for the prison environment. The following information is the manufacturer-provided telephone specifications.

## The Industry Standard

The G-Tel model JP-3600 phones are the overwhelming choice for state prison systems, the Federal Bureau of Prisons, county, and city facilities nationwide because of their proven reliability, durability, and flexibility.

### Features/Options

The proposed phone models include the following features:



- Durable 14-gauge stainless steel
- Built-in mounting plate designed for fast, easy installation
- Mounting plate includes gasket which prevents moisture from entering phone
- Oversized line-wire entrance hole w/ moisture-preventing gasket
- Direct wall- or enclosure-mount
- Tamper-resistant locking system
- Oversized, stainless-steel, ADA-compliant keypad
- Adjustable volume button for full ADA compliance
- Magnetic, sealed hookswitch
- Armored handset cord, with internal lanyard, is made to Bellcore standards and withstands minimum 1000-pound pulling test
- Handset cord retaining bracket is designed for fast, easy handset changes
- Stainless-steel grommet provides added security for the handset cord
- Adjustable handset cord lengths, with standard 24" handset length
- Optional noise-canceling microphone available
- Large, customizable instruction card area
- Tested and compliant with FCC Part 15, Subpart B and ANSI C63.4: 2014 standards. FCC Certificate of Conformity number DL-20171166613C

## EVOTAB TABLET

Unlock a new era with EVOTAB, the pinnacle of tablet innovation, designed solely for the corrections market. As the pioneer in our category, Securus has integrated industry-best hardware and tech-forward features to deliver a device that's redefining what it means to be *corrections grade* and to provide next-level support to your staff. EVOTAB is robust, secure, and user-friendly... revolutionizing the way your Correctional Officers will manage your tablet program and keep your facility safe.



## EVOTAB Conquers Tough Environments.

While other tablets on the market may meet some durability and toughness criteria, our EVOTAB is specifically crafted for hardened spaces. Securus has engineered EVOTAB to withstand even the harshest situations.

- **Deters unauthorized access and intentional damage** with a single-mold, no-screw design and tamper-resistant assembly.
- **Resists dust and water** with IP52-rated tablet construction and an IP68-rated headphone jack, ensuring reliability and quality audio in even the most challenging conditions.
- **Provides safety from drops and impacts** with a TPU of shore hardness 85 type A and TPU bumpers that make cleaning the device easy and eliminate the need for additional protective cases.
- **Withstands high-frequency use** with a rugged design, including sculpted ribs providing improved grip and durability.

## EVOTAB Improves Safety and Security.

This tablet offers the most robust security and safety features available in the corrections technology market. We've designed our device with built-in, top-tier security features including tracking, chirping, and tamper detection alerts to help your staff be more efficient. EVOTAB:

- **Utilizes a proprietary, secure operating system** built off the Google-Certified Android Enterprise platform and backed by Google Security services.
- **Offers authorized device access** through the power button that doubles as a biometric fingerprint scanner to help prevent PIN sharing and serves as an alternative to facial/photo recognition verification.
- **Identifies unauthorized device tampering** with an audible "shriek alarm" when device interference is detected.
- **Mitigate against network tampering** with alerts sent directly to staff if networks are manipulated.
- **Locks devices down automatically** using a tamper circuit that bricks the tablet if the secure device enclosure is breached.
- **Delivers simple tablet tracking and monitoring** with built-in GPS functionality.
- **Helps you locate a tablet easily** by triggering an auditory alarm – even when the tablet is offline.
- **Safeguards against device fraud**, with no external ports, reducing the risk of connecting unauthorized cords or devices.

- **Controls features**, such as Securus Video Connect, are available within certain areas of your facility.
- **Connects to Officer T80 tablets** to provide seamless tablet monitoring and administration for your officers, enhancing safety and compliance.

### EVOTAB Delivers Tech-Forward Hardware.

This device brings you the latest in regulatory-compliant incarcerated tablet technology, including:

- **An improved user experience** with a large 8-inch HD, in-plane switch touchscreen display that makes engaging with tablet content more satisfying for your population.
- **More space for content** with 64 GB of storage (*two times* the storage capacity of our JP6s) so users can download more messages, photos, and media to their devices.
- **Top-speed tablet performance** with 3 GB of RAM – *five times* faster than our JP6s.
- **Enhanced tablet processing** with an Octa-Core central processing unit (CPU) chip.
- **Extended battery life** – up to 8 - 12 hours of constant usage.
- **Multiple connectivity options** through a local network and 4G LTE.
- **Tracking and controlling tablets** with Bluetooth, NFC and GPS.
- **Fully compatible with Officer T80 tablets** to provide an end-to-end solution that is customizable to your unique needs.



### EVOTAB in Action

How can EVOTAB help you mitigate risk and solve critical problems within your facility? Let's explore some common issues and how EVOTAB addresses them.

#### SCENARIO 1: Tablets can't withstand the corrections environment.

**Problem:** Tablets aren't durable enough and are breaking down due to continuous use.

**Solution:** EVOTAB redefines *corrections-grade* technology and is engineered to withstand even the most challenging environments.

- The IP52-rated tablet construction and IP68-rated headphone jack make the EVOTAB dust- and water-resistant.
- A rugged design and sculpted ribs help improve grip, helping to prevent drops.
- TPU of shore hardness 85 Type A and TPU bumpers ensure the tablet is impact-safe without the need for a protective case.
- The single-mold, sealed design makes the tablet easy to clean.
- An improved SIM-shaped pogo pin eliminates confusion between charging ports and headphone jacks, preventing accidental device damage.

### **SCENARIO 2: Incarcerated individuals are physically damaging devices and using them inappropriately.**

**Problem:** People are tampering with tablets, trying to hide contraband inside them, using device parts as weapons, or using their power cables to charge contraband devices.

**Solution:** EVOTAB is built tough and is resistant to even the most extreme device tampering attempts.

- A single-mold, no-screw design makes device tampering unlikely.
- If tampering is detected, an audible “shriek alarm” will sound so your staff can quickly identify and confiscate the tablet.
- The tablet will brick itself and become unusable if the device enclosure is breached.
- A SIM-shaped pogo pin with intelligent power connection limits charging misuse and blocks the ability to charge contraband devices.

### **SCENARIO 3: Incarcerated individuals are attempting to manipulate the tablet software or the network.**

**Problem:** People are trying to hack the tablet operating system or leverage a Wi-Fi connection to access the internet or participate in nefarious activity.

**Solution:** EVOTAB leverages multi-layered operating system security protocols.

- Our proprietary OS is built off the Google Certified Android Enterprise platform, using the highest safety and security standards to mitigate hacking.
- EVOTAB delivers advanced defense against vulnerabilities through anti-exploitation protocols.
- Devices are backed by Google Security services that continuously scan and block malware threats.
- If network tampering is detected, your staff will receive automatic alert notifications.

#### **SCENARIO 4: Tablets are lost or stolen.**

**Problem:** Tablets are missing from inventory, so people are intentionally hiding them, they have been lost, or they have been stolen.

**Solution:** EVOTAB makes it easy for your staff to locate tablets.

- Built-in Bluetooth, NFC and GPS allow your staff to track, in real-time, the exact location of every tablet in your program.
- Staff can trigger an auditory alarm to help locate missing tablets.
- GPS and alarms function even when a tablet is offline.

#### **SCENARIO 5: Incarcerated individuals are sharing credentials and devices.**

**Problem:** Multiple people are using the same login and tablet, making it difficult for staff to manage authorized device access.

**Solution:** EVOTAB security ensures that only the user who is assigned to a tablet can access it.

- The power button doubles as a biometric fingerprint scanner to mitigate against PIN sharing.
- The fingerprint scanner also provides an alternative to facial recognition verification.

EVOTAB empowers your corrections staff *and* your incarcerated population with secure, reliable technology that supports rehabilitation and revolutionizes the industry.

We invite you to join us in shaping the future of corrections technology... exclusively with EVOTAB.

## EVOTAB SPEC SHEET

Daily Usage of Device	8-12 Hours
<b>Product Details</b>	
Form Factor	8" Tablet
Flame-Retardant	UL94 V-1 or Above
Body Structure	1-Part
<b>Processor Details</b>	
CPU	Qualcomm Snapdragon CPU
Clock Speed	Up to 2.4 GHz
Cores	Octa Core
<b>Display</b>	
Resolution	1280 x 800
Touch Panel Type	Capacitive, Gorilla Glass 5
Refresh Rate	60 Hz
Colour Gamut	16.7 M
<b>Sensors</b>	
Ambient Light Sensor	Yes
Gyroscope	Yes
Accelerometer	Yes
Barometer	Yes
<b>Interface/Connector/Options</b>	
Charging Port	5.1 mm Barrel Connector Type
Audio Port	Standard 3.5 mm
<b>Connectivity</b>	
Cellular	4G, LTE
WiFi	802.11 a/b/g/n/ac 2.4 GHz 5G Hz
FM Radio	Yes
<b>GNSS</b>	
GPS	Yes, Dual Band
AGPS	Yes
<b>Memory &amp; Camera</b>	
Internal Storage Capacity	64 GB
RAM	4 GB
Front Camera	5 Megapixel with Auto Focus
<b>Battery and Charger</b>	
Charging Type	Quick Charge
Battery Type	Li-Pol
Battery Capacity (Minimum/Typical)	5000/5100mAh
<b>Biometrics</b>	
Fingerprint ID	Yes
<b>Integrated Accessories/Technology</b>	
Charging LED	RGB
<b>Industry-Based Features</b>	
Antimicrobial Coating	Yes

## EVOTAB Terminal



Concept Only, Design and Product Not Final

### Software features include:

- Current and future EVOTAB apps and functions are supported, including VRS, SVC, outbound Videograms, and mirrors the same, familiar log-in process as the EVOTAB Tablet.
- Portrait mode is available for all applications while remaining ADA compliant.
- Customizable permissions allow facilities to limit specific applications or disable the entire terminal.
- Manage scheduled video visitations with the Conflict Management feature to facilitate transitioning inmates off a terminal before a scheduled video visitation is to start. Controls are configurable based on facility preference.
- Flexibility in data and power options including data over ethernet, power over ethernet, and active secure Wi-Fi networks.

**Providing easy-to-access and easy-to-maintain technology solutions:** With our solutions, onsite Securus administrators can replace terminals while maintaining security

standards. Plus, with 24x7x365 secure monitoring supported by Securus staff, our solutions are safe, reliable, and protected.

## Communication Center

Sedgwick County can operate more efficiently and effectively by replacing manually processed paper forms from Inmates with an end-to-end electronic workflow through Securus' Communication Center. The Communication Center is a custom workflow tool that makes your grievance or form process paperless and allows Sedgwick County staff to process grievances. This application creates staff efficiencies and saves your prison/jail time, paper, and resources.

We lead the corrections industry with ever-improving technology and solutions, including the functionality for Inmates to submit and track various forms.

In addition to various forms, Securus can replicate any detailed problem resolution process that may require appeals, various levels of staff approvals and replies, and specific functionality so that the process supports Sedgwick County's policies.

Forms are submitted via the tablet and each unique submission receives a unique identifier to align the process between Inmate and staff. After submitting the form, the Inmate can track the form process, view replies, and perform other actions such as replying or appealing if specified.

From the staff side, each user has individual access rights so that they can view and respond to the specific forms. Within the system there are also several specific functionalities unique to the staff, such as comments and categorizations not shown on the tablet, detailed search and reporting, and the option to add attachments.

The screenshot shows a mobile application interface for a 'New Communication'. At the top, the status bar displays 'DANIEL SANCHEZ Mon, Mar 2, 20' and the time '5:25'. Below the status bar is a yellow header with a speech bubble icon and the text 'New Communication'. A yellow banner below the header contains the instruction: 'Please verify all your information is correct, then tap SUBMIT.' The main form area has several sections: 'Grievance' and 'Program Services' are dropdown menus. Below them is a section titled 'Enter Details' with a text input field and a character count '550 characters left'. This is followed by 'Date of Incident' with a date picker, 'Action Requested by Inmate' with a text input field, 'Advisor Requested' with a text input field, and 'Steps Taken by Inmate to Resolve Issues' with a text input field. At the bottom right of the form are two buttons: 'CANCEL' and 'SUBMIT'. The bottom of the screen shows the standard Android navigation bar with back, home, and recent apps icons.

## Facility Grievances Interface

Welcome mklunder1@SECUR TXI-302805  
Last Login: 02/15/2021 9:48PM EST

Communications

Assigned To Me (0)

New (12475)

Urgent (0)

Pending (7653)

Awaiting Response (1123)

Appealed (7)

Closed (425836)

Search

Reports

Communications Submitted Report

Create Communication

Communication Response Report

Print Communications

Restrict Inmate Form Use

Inbox: New

Export to file

Page 1 of 176

Filter by Forms:	Inmate Letter	Sort by:	Date (Newest - Oldest)	Filter by Location:	All PermLocs	Filter by Housing:	All Housing
Ref.#:	<a href="#">AZA340000447159</a>	Inmate:	<a href="#">Gomez, Adan F.</a>	Form:	Inmate Letter	Subject:	Transfer Requests
Created:	2/15/2021	ID#:	<a href="#">298103</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	A34 WG3B641B				
Ref.#:	<a href="#">AZM520000447158</a>	Inmate:	<a href="#">Munoz, Patrick</a>	Form:	Inmate Letter	Subject:	Classification/Time Computation
Created:	2/15/2021	ID#:	<a href="#">215284</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	M52 BL2FF14L				
Ref.#:	<a href="#">AZW050000447156</a>	Inmate:	<a href="#">Murabito, Cody W.</a>	Form:	Inmate Letter	Subject:	Banking
Created:	2/15/2021	ID#:	<a href="#">316701</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	W05 HU02B20L				
Ref.#:	<a href="#">AZA340000447154</a>	Inmate:	<a href="#">Johnson, Jason M.</a>	Form:	Inmate Letter	Subject:	Safety
Created:	2/15/2021	ID#:	<a href="#">161509</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	A34 WG3B537U				
Ref.#:	<a href="#">AZA340000447153</a>	Inmate:	<a href="#">Moreno, Albert A.</a>	Form:	Inmate Letter	Subject:	Transfer Requests
Created:	2/15/2021	ID#:	<a href="#">343313</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	A34 WG3B641U				
Ref.#:	<a href="#">AZS060000447152</a>	Inmate:	<a href="#">Bejarano, Gilbert F.</a>	Form:	Inmate Letter	Subject:	Staff
Created:	2/15/2021	ID#:	<a href="#">167825</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	S06 2401C12T				
Ref.#:	<a href="#">AZL210000447151</a>	Inmate:	<a href="#">Mendoza, Roy G.</a>	Form:	Inmate Letter	Subject:	Banking
Created:	2/15/2021	ID#:	<a href="#">050778</a>	Description:	See Subject Above		
Time Left:	27 d	Loc./Hou.:	L21 HU3A511L				

Prior to turning on any form, Securus will provide detailed training to both Inmates and staff, as desired. User guides can also be provided—as needed—to assist the various staff members using the system.

Overall, the top benefits of moving to the Securus digital problem resolution form include:

- Reduced staff time to track down and follow up in person on form progress. Overall, this saves Sedgwick County both money and time.
- Additional access for all Inmates via the tablet, including those using the free option, so they can submit over Wi-Fi
- Enhanced auditing of all system users for increased staff and Inmate accountability
- Enhanced tracking of a form throughout the process, from its submission to the time the form is closed
- Detailed reporting options with multiple ad hoc report options within our tools; Securus will also work closely with Sedgwick County to create customizable reports and dashboards to present the latest information in an easily accessible manner
- Customizable to allow for all forms and processes to fit into the solution

## Functional Overview

The Communication Center electronically processes a **wide variety of forms and communications submitted by Inmates.**

At a summary level, it provides the following functions:

**Securus Technologies**

- Form tools to create and manage multiple form types, each with its own customized workflow
- A user interface for Inmates to:
  - View a list of available form types for completion
  - Complete and submit a form type
  - View a list of their submitted forms and their statuses
  - View the resolution provided to a specific form and either Accept or Appeal the resolution
- An intuitive user interface for facility staff to:
  - View forms awaiting their action
  - Read and assign a form to another staff member for resolution
  - Request more information from the Inmate about a submission
  - Provide a resolution to a submitted form back to the Inmate
  - Establish velocity restrictions to limit form submission abuse
- Options to allow appeal levels to the workflow
- The ability for staff supervisors to:
  - Receive reports of the volumes and progress of forms through the workflow
  - Receive data charts representing age of forms currently in the workflow
  - Assign staff members to process specific forms
- An audit trail of all actions and form responses in the workflow
- Storage and retention of all forms

## Application Overview

The Communication Center allows Sedgwick County to replicate their existing paper forms in an electronic format.

Examples of forms include the following:

- General Grievance
- General Request
- Anonymous Grievance
- Request medications
- Request Law Library Access

- Request Sick Call
- Tablet Self-Help

## Form Capabilities

Key form capabilities include the following:

- Text fields are automatically filled using the NextGen SCP data, e.g., Custody Account Number
- Text fields entered by the Inmate
- Text fields entered by facility staff that can be configured to be hidden or viewable by Inmate
- Check boxes and other multi-select tools configurable by form
- Pre-formatted styles used to set the fields' location and format on the form
- Work-flow unique to the form type
- A General Grievance could have a workflow with multiple Appeal Levels, while a request for Law Library Access could have no Appeal level

## *Authenticated and Anonymous Forms*

### **Authenticated Forms**

Authenticated Forms require an Inmate to log in prior to completing the form. The Grievance application attaches the Inmate's identity to the form for the visibility of facility staff. Optionally, Inmates can be required to re-authenticate to submit forms.

### **Anonymous Forms**

An "anonymous form" does not require the Inmate to log in to the Inmate Forms and Grievances Application. The Inmate Forms and Grievances application does not attach the Inmate's identity to the form to protect Inmate from possible recrimination. Anonymous forms have no means by which the Inmate may protest (escalate) the resolution of the form. Therefore, anonymous forms cannot have escalation levels.

Because anonymous forms have a simpler workflow than authenticated forms, they can be used as a light-weight processing of forms. Anonymous forms could be used to capture and process simple requests that do not need a response to be sent back to the Inmate.

Because the Forms and Grievances Application does not track the identity of the Inmate submitting an Anonymous form, the form can ask the Inmate to provide their name and/or custody account number.

Anonymous forms can be accessed by Inmates whose PINs are inactive and are restricted from using the phone system.

### *Appeals/Escalations*

One or more appeal or escalation levels can be configured for each form. Simple requests typically do not have appeal levels configured. Formal grievance forms can have one or more levels depending on the facility's existing grievance process.

### *Velocity Restrictions per Form Type*

Adjustable velocity restrictions limit the number of times that an Inmate can submit a particular form to minimize abuse. After the limit has been reached, the application blocks the Inmate from creating more forms of that type until the next time interval.

### *Form Categories*

Form categories provide users the ability to categorize the forms listed on the Inmate Forms and Grievance application.

### *Auto Resolve Capability*

Auto-Resolve is a configuration that allows a form to automatically resolve itself if an Inmate is either released or transferred from the facility prior to the completion of the form.

## **Video Relay Service**

Securus' NextGen SCP™ provides support for hearing-impaired inmates through both Video Relay Service (VRS) and TTY/TDD. The Securus VRS solution is a complete solution for correctional-grade VRS services that incorporate FCC regulations, as well as the inmate call controls, management, and investigative abilities expected for inmate calls.

VRS offers unique challenges to the correctional industry due to its reliance on American Sign Language (ASL), which requires visual communication, the automatic insertion of an ASL interpreter when needed, and adherence to FCC regulations that prohibit VRS service providers from interfering with or recording the communication.

Securus VRS addresses all these challenges so as to provide Sedgwick County with a VRS solution that does more than meet the requirements of ADA compliance—Securus VRS meets these challenges through a high-level integration with NextGen SCP. The high level of integration between Securus VRS and NextGen SCP provides hearing-impaired inmates with “equal access” to communication services while allowing Sedgwick County to provide, manage, and investigate inmate VRS calls in a manner consistent with traditional inmate calls.

Securus VRS provides equal access by allowing Sedgwick County to:

- Provide VRS-capable inmate call devices that fully conform to the rigorous needs of the correctional environment
- Manage VRS calls using the same controls as are used for traditional inmate calls
- Record VRS calls in accordance with the same recording controls that govern whether to record traditional inmate calls
  - Securus VRS can record VRS calls because Securus is not a “VRS Provider”. Instead, Securus is partnered with ZVRS/Purple to be the “VRS Provider”. The nature of this relationship, along with the proprietary integration of technologies, allows NextGen SCP to record VRS calls while remaining compliant with FCC regulations.
- Include VRS call recordings in investigations including inclusion in CD images and individual downloads.



Securus VRS call recordings include the visual component of the inmate call for both the inmate and the other end of the video portion of the VRS call. The other end of the VRS call might be the inmate’s called party (if they are a registered subscriber to the public VRS service) or the VRS interpreter (if the called party is not a registered subscriber to the public VRS service). Since the public VRS service automatically bridges in a VRS interpreter when necessary, Securus VRS fully accommodates the various scenarios the public VRS service may encounter. These scenarios include the potential that a VRS Service provider supports Voice Carry-Over (VCO). When VCO is supported, the Securus VRS call recording will include the audio component of the VRS call.

Our VRS uses the same standard inmate call management control structures as for traditional inmate calls, including the following call controls:

- Calling schedules
- Max call duration controls
- Calling Restrictions
- Calling Velocity
- Called party phone number control—both globally and on inmate PAN lists
- Call recording
- Collecting VRS calls in inmate calls for investigations and evidence

This level of integration between Securus VRS and NextGen SCP means that Sedgwick County can set inmate calling policies that apply equally to all inmate calls, including VRS calls, or set unique policies for VRS calls.

Inmate access to Securus VRS is provided as an application available through our devices.

Because VRS calls are required by the FCC to be free, all inmate VRS calls will be provided at no cost to the inmate. To ensure Sedgwick County can prevent the unauthorized use of Securus VRS to place free calls, the Securus VRS is also integrated with NextGen SCP to allow Sedgwick County to designate which inmates are allowed to place VRS calls. The Securus VRS application requires inmates to enter their designated inmate ID and their calling PIN before placing calls. To accommodate the needs of the hearing-impaired, Securus VRS can be configured to work without PINs in designated booking and/or intake areas. With these controls, Sedgwick County has security over VRS calling as well as the flexibility to allow VRS calls in situations where detainees have not yet been issued a PIN.

Securus VRS represents the ultimate solution for accommodating conformance to ADA compliance and FCC regulations, and the necessary call controls and investigative abilities to ensure safe communications.

## Carts / Portable Sets

We will provide a roll-away phone mounted to a roll-around pedestal, in a four-wheel design or a two-wheel design, as shown.

The phone can also be mounted to a hand truck (dolly).



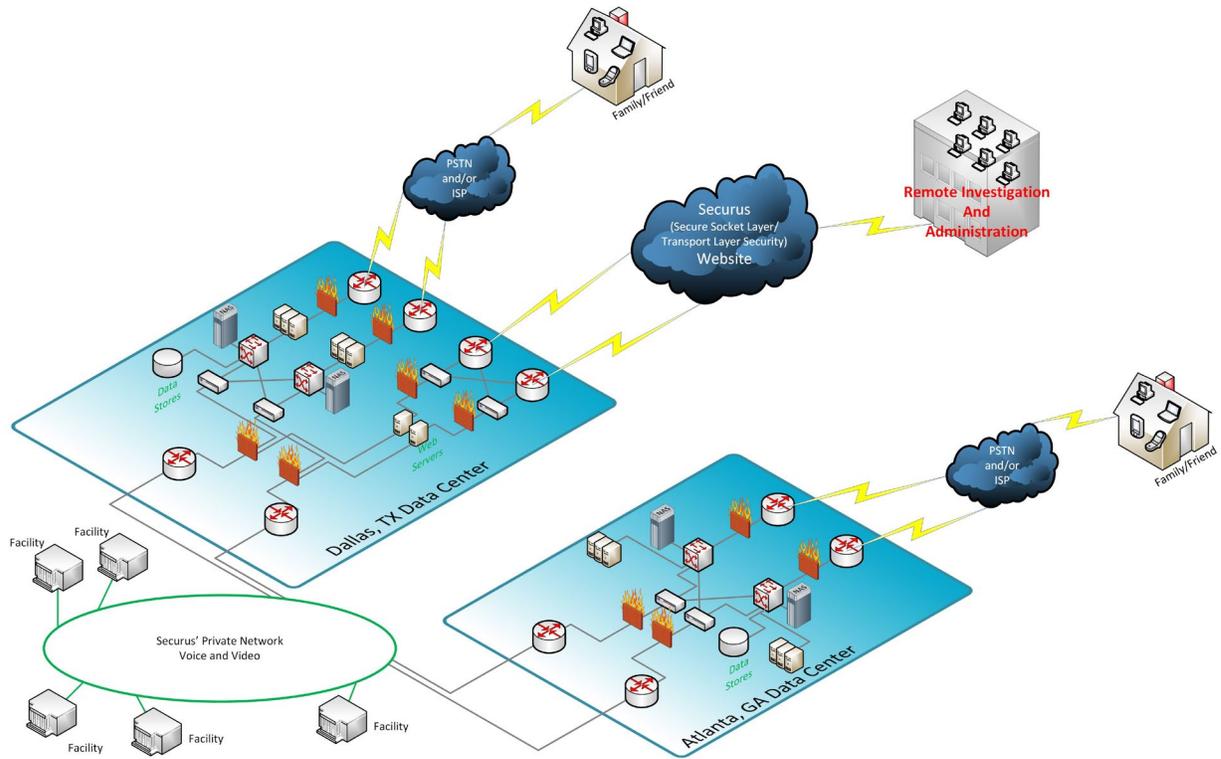
## SYSTEM ARCHITECTURE AND DESIGN

### 1. System Diagram

**Provide a diagram of the proposed system architecture. The diagram should include an overall representation of the servers, network, peripherals, workstations, mobiles, and interface points, as well as a representation of the system environments (Production, Test, Training, and Disaster Recovery) and their interdependencies.**

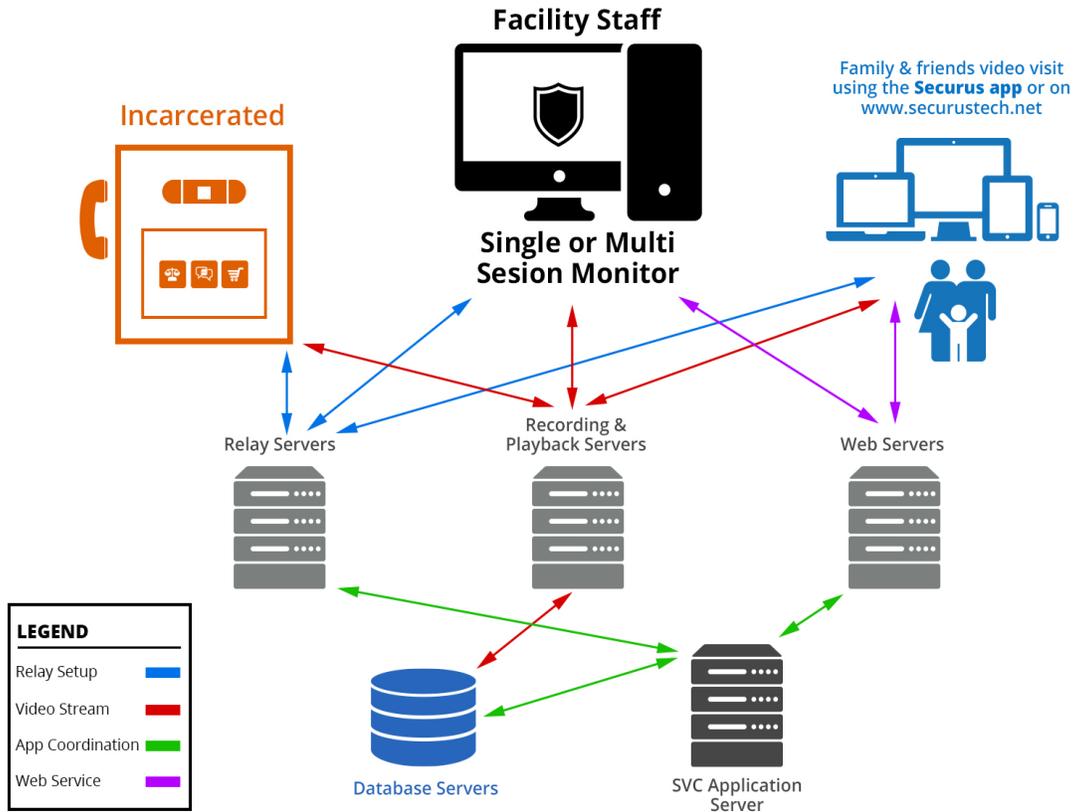
## SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. -

Below is a diagram showing the secure transfer of data to and from Sedgwick County Detention Facility.

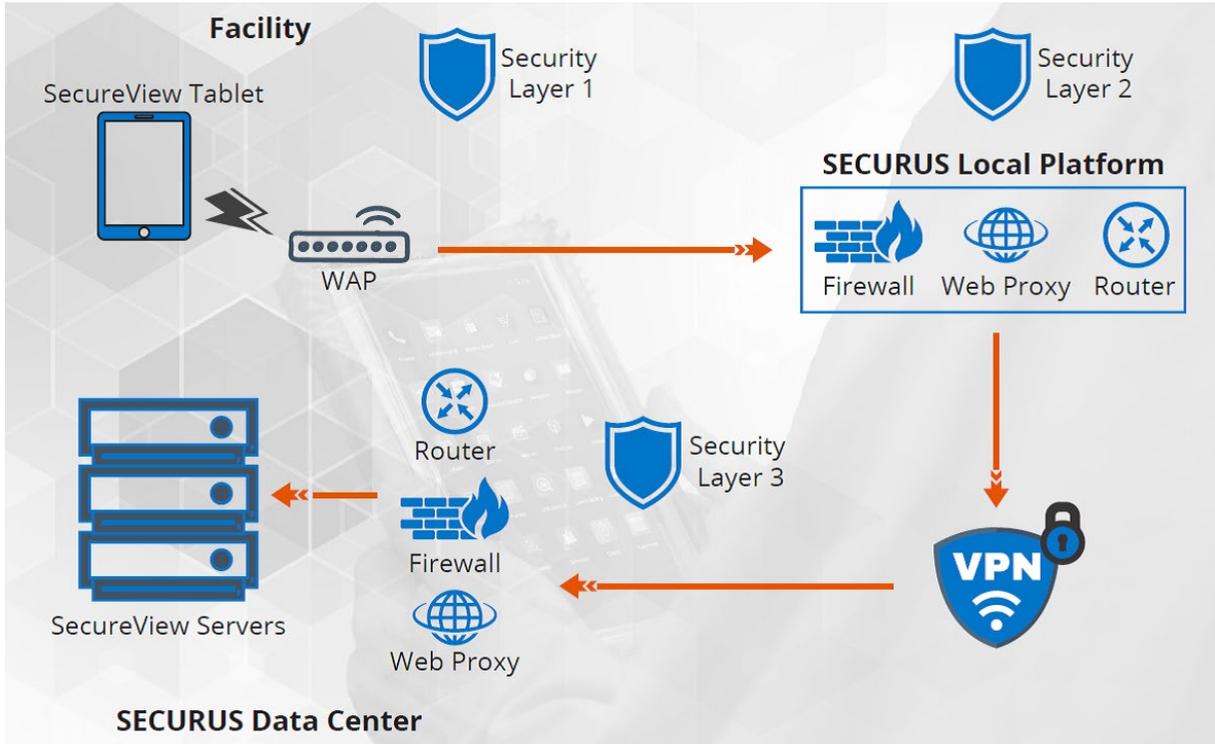


Below is a diagram of how inmates, Sedgwick County staff, and family and friends interact with each other through the SVC system architecture.

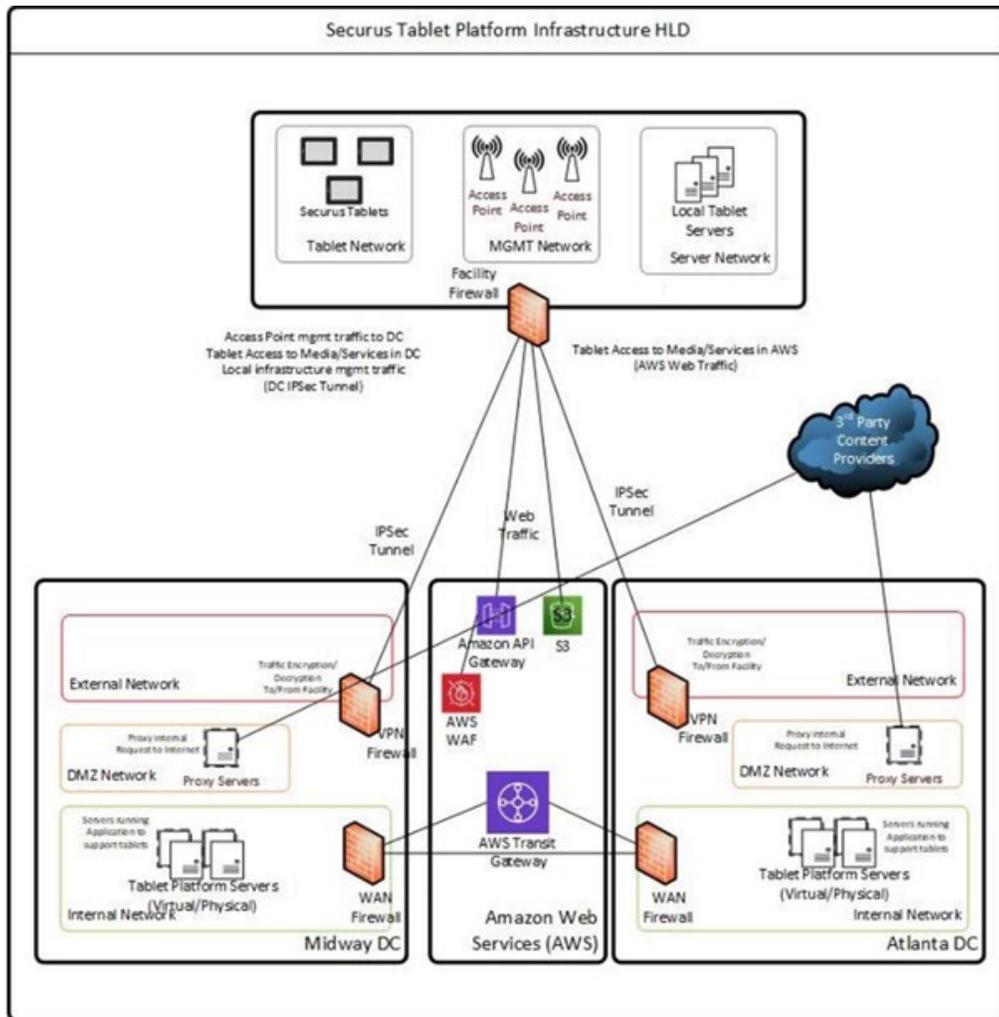
## SVC SERVER ARCHITECTURE - XL



Below is a diagram of how tablets interact with the network to ensure a layered security system.



## Securus Tablet Platform Infrastructure HLD



## Disaster Recovery

Our Disaster Recovery Plan is designed for rapid response with unmatched service and support in any circumstance. Our goal is to prevent or minimize down-time and remove your administrative burdens. **Securus takes care of communications and technology while you take care of your population and facilities.**

- Robust network architecture designed to mitigate issues before they occur
- Field service team readily positioned close to your facilities and on-call 24/7
- A plan for escalating issues, adding resources, and recovering quickly

If a natural disaster or other significant adverse event occurs, Sedgwick County has the full support of the Securus Network Operations Center, the Securus Technical Support

Team including engineering resources, and the Securus Field Service Team supported by a centralized field dispatch team. Our Field Service Technicians are fully trained in our disaster recovery plan and processes, and they are strategically positioned to support your ongoing maintenance and fast response in emergencies.

Response operations begin as soon as personnel safety is assured, and all emergency recovery operations are prioritized by critical facilities and equipment locations. For situations that are expansive in nature, we prioritize maximum-security sites and facilities with high offender phone usage.

## Three-Tiered Approach to Disaster Response and Recovery

### 1. Facility-Specific Emergency Response Checklists

For every facility, we develop an emergency response checklist to protect equipment and personnel in the event of an emergency. These procedures may be as simple as using sandbags to stabilize equipment and placing tape on windows exposed to high winds. Your checklists will focus on mitigation and recovery with contingencies for extreme conditions such as earthquakes, flash floods, power outages, etc. Each checklist will be coordinated with Sedgwick County for consistency with your policy and procedures.

### 2. Systemwide Disaster Response Plan

Securus works with you to declare emergencies for situations that are catastrophic and may impact a localized area or wide-spread region. Recovery plans are triaged based on the extent of impact and recovery operations may last a few hours, days, or weeks. Securus prioritizes recovery of premise-based equipment by facility type and equipment location. The Securus Local Recovery Team will continue recovery operations until operations are restored. Retrospective reports are completed for all declared emergencies to advance our emergency recovery planning efforts for the future.

### 3. A Foundation of Network and Equipment Preventative Measures

Sedgwick County **avoids many communications-related disasters because we are prepared:** Securus provides a network and infrastructure tested to withstand adverse conditions, minimize outages, and protect your data. We research what works and then we implement continuous improvements. Securus adds layers of redundancy at the local and national level to our core network and operations centers. We stock your facility and our Field Service Team with spare parts. We back up your data at three geographically diverse Securus data centers and layer redundancy throughout each component of our network. Information is routed through geographically diverse and route-diverse network paths, all while we monitor operations and communications 24x7x365.

Additional details on the Securus Disaster Recovery Plan and our preventative measures are outlined on the following pages. It's difficult to contemplate every contingency, but with 30+ years of experience providing communications and technology services to the corrections industry, **Securus has the experience to take care of Sedgwick County even when the unexpected occurs.**

### Sedgwick County Emergency Condition Declaration

**If you encounter a catastrophic adverse event or disaster at your facility, immediately call the Securus Emergency Numbers** that you are provided. Your call will be answered 24x7x365. Then with your Securus Account Manager you will request that Securus General Manager declare an emergency condition. Operations management then establishes an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determines the Disaster Level.

Securus classifies disasters on a Disaster Level Scale of 1-3:

- Level 1 Disasters are catastrophic events that are extremely wide-spread and affect many facilities and many customers.
- Level 2 Disasters are high-impact and affects a more wide-spread area than Level 3.
- Level 3 Disasters are moderate impact disasters typically affecting a localized area or specific facility with consideration that elevation of level may be needed.

**A single event trouble ticket is used to track all recovery efforts.** The Securus Technical Support Team will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked so that all recovery efforts are tracked as a single incident to facilitate complete resolution. This is critical for efficient and complete resolution in situations of extended recovery.

**If needed, Securus will deploy and pull resources from our nationwide network and engage our vendors to supply additional resources, equipment, or manpower.**

## EMERGENCY RESPONSE DISASTER LEVELS

### Disaster Level 1

Securus provides a full-headquarters response and may deploy a Headquarters Response Team to the region to coordinate and assist local recovery efforts. Securus Local Recovery Team activated, and your Account Manager will work with you to initiate a Command Center, including Securus Leadership. Necessary skill levels and geographic proximity are matched to your site's needs; additional personnel are dispatched as needed.

### Disaster Level 2

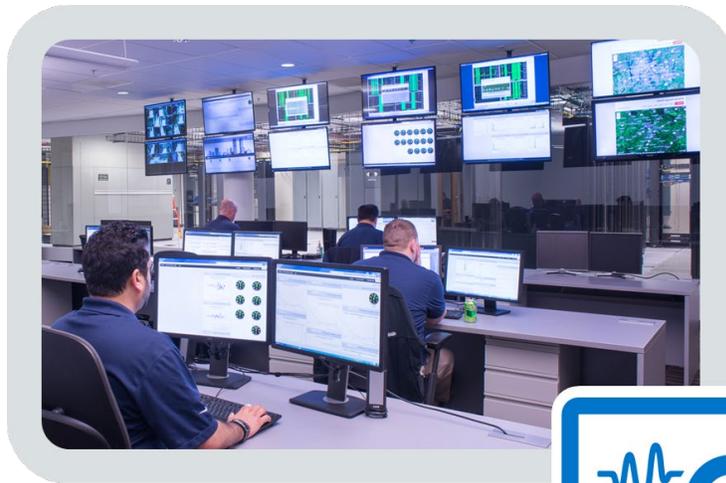
Securus Headquarters Response Team assists Securus Local Recovery Team as needed; onsite technician requirements assessed, and additional personnel dispatched as and when needed.

### Disaster Level 3

Securus Local Recovery Team coordinates all recovery operations. Headquarters assistance beyond standard Network Operations and Technical Support Teams likely not required.

## Risk Mitigation and Proactive Monitoring

**The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems** using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.



**SECURUS' NETWORK OPERATIONS CENTER**



The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, **Securus maintains a fully redundant backup Network Operations Center at a separate physical location.**

**The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365** including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

**The systems are polled every two minutes and their vital operating statistics sent every 10 minutes.** In addition to real-time monitoring and alerting, Securus Technical Support also leverages network performance monitor tools to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

**Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan.** Securus maintains three data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.

Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security

- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

**Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.**

**Data is no longer susceptible to loss due to an individual drive failure or issues at your location:** The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provides facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on your site, in our Field Service Team vehicles, and at centralized locations.** In addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

### Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

## 2. Proposed Hardware Configuration

**Provide a listing or description of hardware configuration(s) recommendations based on use experience.**

Since Securus uses multi-tenant systems, hardware and resources are scaled as needed to meet all of Sedgwick County's needs.

### EVOTAB Tablet Hardware

Securus offers the following tablet hardware specifications.

#### Incarcerated Individual Tablet

The Securus EVOTAB tablet hardware incorporates the following features and specifications.

The following table lists the complete EVOTAB specifications.

Daily Usage of Device	8-12 Hours
<b>Product Details</b>	
Form Factor	8" Tablet
Flame-Retardant	UL94 V-1 or Above
Body Structure	1-Part
<b>Processor Details</b>	
CPU	Qualcomm Snapdragon CPU
Clock Speed	Up to 2.4 GHz
Cores	Octa Core
<b>Display</b>	
Resolution	1280 x 800
Touch Panel Type	Capacitive, Gorilla Glass 5
Refresh Rate	60 Hz
Colour Gamut	16.7 M
<b>Sensors</b>	
Ambient Light Sensor	Yes
Gyroscope	Yes
Accelerometer	Yes
Barometer	Yes
<b>Interface/Connector/Options</b>	
Charging Port	5.1 mm Barrel Connector Type
Audio Port	Standard 3.5 mm
<b>Connectivity</b>	
Cellular	4G, LTE
WiFi	802.11 a/b/g/n/ac 2.4 GHz 5G Hz
FM Radio	Yes
<b>GNSS</b>	
GPS	Yes, Dual Band
AGPS	Yes
<b>Memory &amp; Camera</b>	
Internal Storage Capacity	64 GB
RAM	4 GB
Front Camera	5 Megapixel with Auto Focus
<b>Battery and Charger</b>	
Charging Type	Quick Charge
Battery Type	Li-Pol
Battery Capacity (Minimum/Typical)	5000/5100mAh
<b>Biometrics</b>	
Fingerprint ID	Yes
<b>Integrated Accessories/Technology</b>	
Charging LED	RGB
<b>Industry-Based Features</b>	
Antimicrobial Coating	Yes

## NEXT GEN OFFICER TABLET

Securus is uniquely positioned to solve the technical challenges faced by customers in the correctional landscape. Our new Officer T80 tablet stands as a beacon of innovation and precision, addressing facility needs with best-in-class efficiency and foresight.

## **Achieve Unmatched Flexibility and Control.**

Our T80 tablet ecosystem offers unparalleled flexibility and control, allowing seamless integration of Securus applications alongside apps from a managed, private Google Play store. You can customize each tablet to meet your agency's specific needs, with support for multiple user profiles, as well as connectivity options.

## **Get Google-Certified Security.**

By transitioning our officer tablet to the Android Enterprise platform certified by Google, Securus is able to provide tablet security with the highest security standards. Using a device that is Android Enterprise-certified provides a robust and comprehensive security framework backed by Google's safety expertise. From over-the-air patches to malware detection, our Officer T80 tablet protects sensitive data, mitigates risk, and maintains a secure environment that helps you keep your staff and population safe.

## **Experience Cutting-Edge Hardware**

You'll hold the latest in corrections tablet technology in your hands with our Officer T80 tablet. Featuring an 8-inch HD touchscreen, 3GB of RAM, 32GB of storage, extended battery life, and built-in GPS, our Officer T80 device is five times faster than our previous model and is built to withstand the demands of modern correctional facilities.

What's more, our T80 officer tablet is tailored to help you solve business critical issues by bridging the gap between technology, staffing and operations.

Here's how our latest offer tablet solution will transform the way you work.

## **Add Flexibility to How You Administer Your Tablet Program.**

Since our T80 officer tablets leverage an LTE connection, you can manage any active device that's part of your tablet program without actually having to be connected to the local site. This means that you're able to control your devices from anywhere – your agency headquarters, inside a different facility, or even at home!

## **Streamline Operations.**

By offering you the ability to download apps available within our managed, private Google Play store, you can select the pertinent application solutions that help your staff handle policy changes, signatures, incident reporting and other critical tasks. Our T80 officer tablet helps optimize operational workflows, saving you time and resources.

## **Reduce Technology Costs.**

Say goodbye to multiple devices cluttering up your workspace. The T80 officer tablet serves as a comprehensive solution, eliminating the need for supplementary administrative technology such as computers, smart devices, and full workstation setups in housing units. This consolidation reduces the budget required for you to offer a full-service technology suite.

### **Simplify Tech Management.**

With automatic over-the-air updates and robust security management directly from Google, maintaining the T80 officer tablet is effortless. Our full-service tech management solution ensures your staff can focus on essential facility tasks without the burden of constant oversight across multiple devices.

### **Boost Employee Recruitment and Retention.**

By expanding the capabilities of the officer tablet to support non-Securus applications, we empower you to select apps for your staff from a wide array of Google-ready apps we've made available in our managed store. Our T80 officer tablet gives you the ability to enhance staff education and training programs while fostering a supportive work environment.

Revolutionize your correctional operations with the Securus T80 officer tablet. This innovative technology powerhouse will elevate your facility's performance and security standards to help you achieve organizational goals... with a click.

## **EVOTAB Terminal**



Concept Only, Design and Product Not Final

### Software features include:

- Current and future EVOTAB apps and functions are supported, including VRS, SVC, outbound Videograms, and mirrors the same, familiar log-in process as the EVOTAB Tablet.
- Portrait mode is available for all applications while remaining ADA compliant.
- Customizable permissions allow facilities to limit specific applications or disable the entire terminal.
- Manage scheduled video visitations with the Conflict Management feature to facilitate transitioning inmates off a terminal before a scheduled video visitation is to start. Controls are configurable based on facility preference.

**Providing easy-to-access and easy-to-maintain technology solutions:** With our solutions, onsite Securus administrators can replace terminals while maintaining security standards. Plus, with 24x7x365 secure monitoring supported by Securus staff, our solutions are safe, reliable, and protected.

### 3. Performance and Reliability

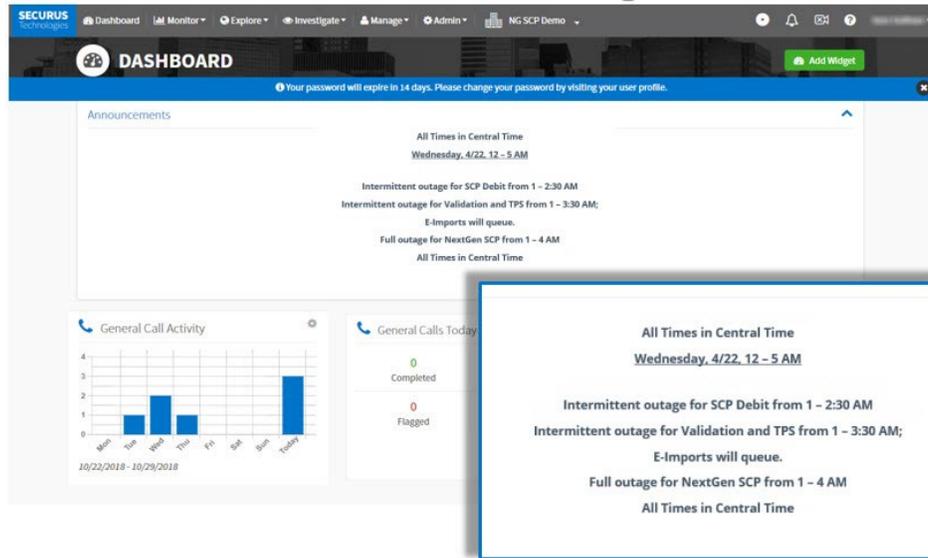
a. Describe any impact to systems (e.g. interference to normal operations, system shutdown) that will occur during server upgrades and/or expansions.

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Current technology provides better support and higher satisfaction:** Securus delivers NextGen SCP software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

**Minimize disruptions to communications and your work:** To deliver updates and perform maintenance events, Securus uses an after-hours process. Sedgwick County will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

## Announcement Widget



SVC is managed through the NextGen SCP, making it easy for us to provide regular updates and feature upgrades.

Updates to EVOTAB Tablets are done wirelessly. These updates include virus protection, application updates/upgrades, and patches, with no need to sync to external hardware. The EVOTAB firmware includes the antivirus protection for the tablets, so there is no need for a separate anti-virus program to be installed. With any new firmware release, it includes updated anti-virus protection.

### b. How will the Vendor ensure concurrent operation of all system components without degradation?

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We continuously monitor all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including the NextGen SCP, network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data

centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

### Securus Primary Network Operations Center



### Securus Network Operations Center



### Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches, and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure,

Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

### Infrastructure Inspections

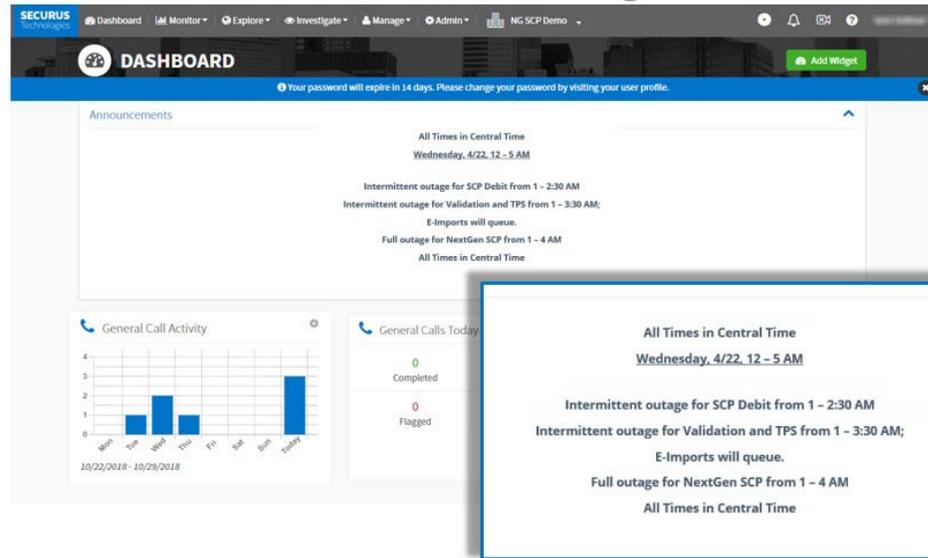
System Administrators make scheduled inspections of all systems and routinely perform preventive maintenance and software enhancements as directed by a Production Change Control steering group. In addition, Securus change control practices have been reviewed and are compliant with PCI DSS and our Internal Controls for Financial Reporting.

## Continuous Software Updates and Minimal Disruptions

**Current technology provides better support and higher satisfaction:** Securus delivers NextGen SCP software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

**Minimize disruptions to communications and your work:** To deliver updates and perform maintenance events, Securus uses an after-hours process. Sedgwick County will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

## Announcement Widget



## Wireless Tablet Updates and Built-In Protection

Updates to EVOTAB Tablets are done wirelessly. These updates include virus protection, application updates/upgrades, and patches, with no need to sync to external hardware. The EVOTAB firmware includes the antivirus protection for the tablets, so there is no need for a separate anti-virus program to be installed. With any new firmware release, it includes updated anti-virus protection.

- c. Describe the system response times that will be guaranteed during the lifetime of the system (both during original warranty period and lifetime support). This is specifically referring to the transaction times related to commands.

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Specifically in reference to transaction times related to commands, Securus guarantees immediate system response times during the lifetime of the system.

- d. Describe how the Vendor will measure and ensure system performance over the lifetime of the system.

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We continuously monitor all data centers, infrastructure components, platform systems, and communications services using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time

monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.

The Securus Network Operations Center (NOC) provides 24x7x365 monitoring for all Securus systems, including the NextGen SCP, network, back-office systems, and data centers. The NOC proactively monitors these systems to ensure performance is optimal and uninterrupted. In addition to system and network-level monitoring, the NOC also monitors real-time video surveillance and environmental alerts for our data centers. Securus maintains a fully redundant backup NOC at a separate physical location, should services be disrupted at the primary location.

### Securus Primary Network Operations Center



### Securus Network Operations Center



## Premise Equipment

The Securus Technical Support team provides 24x7x365 monitoring of all facility-based equipment and directly supports facility installations via telephone and email. Technical Support monitors connectivity for all installations and all installed equipment including Integrated Access Devices (IADs), Visitation Phone Monitoring (VPM) units, switches, and Uninterrupted Power Supply (UPS) systems. The systems are polled every two minutes to ensure proper operation, and their vital operating statistics sent every 10 minutes. Upon receiving an alert indicating network failure, Securus will open a trouble ticket with the appropriate circuit provider. In the case of a premise-based equipment failure, a Securus Field Technician is dispatched to the facility for on-site repair.

In addition to real-time monitoring and alerting, Securus Technical Support also leverages the network performance monitor to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. The detailed level of monitoring available via our network performance monitor allows the Technical Support group to take proactive steps to prevent or mitigate facility outages and to ensure the correct resources are engaged if dispatch is necessary.

## Infrastructure Inspections

System Administrators make scheduled inspections of all systems and routinely perform preventive maintenance and software enhancements as directed by a Production Change Control steering group. In addition, Securus change control practices have been reviewed and are compliant with PCI DSS and our Internal Controls for Financial Reporting.

- e. **The county expects seven (7) days a week, 24 hour operation regarding the solution. Describe how the Vendor will guarantee 99.999% availability both initially and during the life of any license and maintenance contract.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THE DEFINITIONS PROVIDED BELOW.**

We have maintained network and platform availability exceeding our rigorous, standard objective of 99.9%. This objective of 99.9% does not include maintenance windows for regular system maintenance and system upgrades that are performed overnight. An outage is determined when the platform is unavailable for whatever reason. If a call type of any kind can be completed, then the platform is not in an outage situation. With our centralized platform, unplanned system failures or outages rarely occur. Our data centers have redundant connections to power and telecommunications providers, and battery and diesel generator protection. There have been isolated incidents where communication processing was interrupted due

to network failures, hardware failures, or software failures at various points in the network; all were resolved promptly.

We understand the importance of keeping communication available, and the frustration created when interrupted. Telecommunications networks often have issues, but a centralized, proactively monitored platform allows us to respond immediately.

**f. What level of system availability is recommended for the solution?**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our Network Operations Center (NOC) is dedicated to monitoring and measuring the performance of SVC. When outages occur, our NOC staff handles them quickly to limit customer impact to total system failure.

**Annual SVC Uptime Statistics**

	2014 - 2016	2017	2018	2019	2020	2021	2022	2023
SVC User Interface Availability:	99.870% - 99.987%	99.994%	99.943%	100%	99.884%	99.862%	99.952%	100%
SVC Platform Availability:	99.870 - 99.987%	100.00%	99.990%	100%	99.967%	100%	100%	100%
SVC Network Availability:	99.885% - 100%	99.998%	99.997%	100%	99.973%	100%	100%	100%

Securus Calling Service, launched in February 2006, has never experienced a total system failure lasting more than 24 hours. Securus currently operates services at 1,700+ sites and the Securus Network Operations Center (NOC) works around the clock to monitor and measure performance. When an outage occurs, the NOC resolves the issue promptly to minimize downtime and impact.

The following statistics show the most recent Securus Calling Service uptime through 2021.

## Annual ITS Uptime Statistics

	2012 -2015	2016	2017	2018	2019	2020	2021	2022	2023
SCP User Interface Availability	99.828% - 100%	99.995%	100%	99.943%	99.967%	100%	100%	100%	100%
SCP Platform Availability	99.865% - 100%	100%	100%	100%	100%	100%	100%	100%	99.998%
SCP Network Availability	99.885% - 100%	100%	100%	100%	100%	100%	100%	100%	99.998%

Securus Tablets have an outstanding record of performance and uptime demonstrated by years of solid data. The Network Operations Center (NOC) monitors and measures performance 24/7 and if ever there is an outage our response is fast to minimize impact on your facility and population.

## Annual Tablet Uptime Statistics

	2017	2018	2019	2020	2021	2022	2023
Tablet User Interface Availability	99.942%	100.00%	100.00%	100.00%	100.00%	100%	100%
Tablet Platform Availability	100.00%	99.997%	100.00%	99.967%	99.607%	100%	100%
Tablet Network Availability	99.998%	99.997%	100.00%	100.00%	99.904%	100%	100%

g. Describe how the Vendor will guarantee this level of availability both initially and during the life of any license and maintenance contract?

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus provides highly reliable service from initial system design and installation through ongoing maintenance and support. Our service and maintenance program includes integrated remote programming, diagnostics, downloading, and troubleshooting capabilities. Securus does not charge for maintenance, support, training, and repair of system software and equipment.

Our local service and account management teams provide support 24 hours per day, seven days per week, and 365 days per year (24x7x365). The local team of Securus employees have demonstrated their dedication to the counties in the state of Kansas.

The Securus Field Service Team solves technology issues that arise at your site during our contract. **The Sedgwick County system will work with minimal downtime.**

- Rapid response by local field technicians with extensive skills and experience
- Quick access to on-hand replacement parts inventory
- Proactive preventative system maintenance

We have one of the largest Field Service Teams in the industry strategically positioned across the nation for quick response. **Our Field Service Technicians average 7+ years of experience at Securus**, bring an extensive telecommunications background, and are Securus-certified to service all products. In addition, our Field Service Technicians have the support of local Service Managers and Regional Managers, a centralized Field Dispatch Team, a Project Management Team, an Onsite Installation Team, and the Securus Engineering Department. Sedgwick County gets minimal downtime and expedited repairs.

If Sedgwick County identifies an issue, **a call to the Securus Technical Support Center at 1-866-558-2323 will initiate Securus response.** If onsite service is required, the Field Dispatch Team assigns the local Field Service Technician, determines an estimated time of arrival onsite (typically less than two hours), and confirms service time with Sedgwick County. Upon arrival, the Field Service Technician meets with the primary site contact to review the problem. Typical repairs might include repairing or replacing parts, correcting configuration settings, or re-wiring.

**Our Field Service Technicians maintain an extensive replacement parts inventory onsite at your facility and/or on their service vehicle.** Located nationwide, the Securus replacement parts inventory exceeds \$3.5 million, and most repairs are resolved with local, on-hand parts. When additional parts are needed our Team works together to get the supplies to your facility fast.

After the reported issue is resolved, **the Field Service Technician proactively performs a system check to detect additional issues and completes preventative maintenance** including cleaning system filters, testing system features, functionality, and individual units, and workstation inspections. Our goal is to address any additional problems during the same visit when possible. Upon completion of all work, the Field Service Technician confirms satisfactory resolution with Sedgwick County and documents all work for future reference.

Sedgwick County receives a satisfaction survey via e-mail following each service event and, if there is any concern noted, it is addressed immediately. Your local Service

Manager or account representative will contact Sedgwick County promptly to discuss your concern and implement a corrective action plan. As a result of this focus on customer service, Securus customers regularly give high marks in the satisfaction surveys following field service events.

Service policies and procedures that are engineered for minimal downtime and expedited repairs are included in the Securus sample contract included as Attachment E.

#### 4. System Failover and Restoration

##### a. Provide a detailed description of the proposed backup environment.

###### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

NextGen SCP™ is a fully self-contained digital switching system and requires minimal AC power. If local power fails, the uninterruptible power supply (UPS) maintains system power and operations, including recording and network services, for a minimum of 15 minutes. The UPS eliminates spikes, sags, surges, transients, and all other over/under voltage and frequency conditions, providing clean power to connected critical loads.

If there is a local power failure, all calls and video sessions should have time to complete. The Integrated Access Device (IAD)s and UPS maintain all in-progress calls and video sessions for up to 30 minutes while blocking additional call or video attempts after the event. After 30 minutes, the system terminates all communication in progress and powers down to a quiescent state so that the system automatically resumes full operation after the restoration of commercial power.

###### **Uninterruptible Power Supply – Facility Backup**

All UPS equipment provides power conditioning and an additional layer of surge protection. The rack-mount UPS is a high-density backup-power protection solution ideal for servers, storage systems, network equipment, and other critical devices. It also offers the best UPS power protection against five of the nine most common power-quality problems. The slim design and wide range of UPS system installation possibilities make this the most versatile UPS power quality solution available.

Additionally, Securus provides offsite data storage at multiple locations to minimize risks related to localized disasters, power outages, or security breaches. Securus operates and maintains two geographically diverse and fault tolerant carrier class data centers—Sedgwick County data is securely stored offsite. Each data center also has an uninterruptible power supply (UPS), and a generator to provide maximum network uptime.

## Uninterruptible Power Supply – Data Center Backup

Power distribution units (PDUs) distribute power to individual customer racks via remote power panels. Each rack has redundant power strips (A & B) routed to diverse PDUs. Diverse uninterruptible power supply systems feed each power distribution unit.

The UPS systems in our primary data center have 2N redundancy. Dual source power runs through a static bypass switch. Battery rooms support the UPS systems with gel cell battery banks. Fifteen minutes of battery backup is available at full load (such as 90 watts per square foot). Each battery bank is continuously monitored to ensure optimal operation. Upon loss of commercial power for more than 15 seconds, paralleling switchgear automatically powers all nine generators; generators are shed to cover load as needed. Typically, the transition from UPS to generator power takes 60 seconds.

Securus Data Centers each have multiple diesel generators onsite with fuel storage tanks that hold 70,000 gallons onsite. Our generators are tested weekly and provide alerts if there is a test failure. Securus maintains multiple fuel vendor agreements to have flexibility and options for fuel purchases.

- b. Do operations automatically failover to the backup environment in the event of a failure in the production environment? Describe any actions that must be taken by personnel to activate a backup environment.

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

No action is required by Sedgwick County to activate the backup environment.

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

- c. How much time is required until operations commence in the backup environment when operations in the production environment fail?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our backup is continually in place due to our **redundant protection against failures and disasters**: Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

- d. What steps, degree of user intervention, and time is required to return operations to the primary environment?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As soon as commercial power is available, the system will return to the primary environment instantly and automatically.

## 5. Security

- a. What authentication mechanisms do you use?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus uses Microsoft Active Directory version 88 to manage user authentication to access NextGen SCP. This version of MS Active Directory is compatible with LDAP versions 2 and 3. All user credential authentication is performed against this system. At this time, we do not integrate with any external LDAP systems.

- b. Do you support SAML or syncing with Azure AD? If you don't support SAML, do you have your own two (2) factor authentication?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. -**

NextGen SCP is a centralized, digital network that is accessed via the web by navigating to <https://ngscp.securustech.net> in the supported browser, Chrome.

The platform is protected by SSL (secure socket layer) security, which uses the same security protocols that banks use for establishing a connection for customer online banking.

- c. Do you have the ability to restrict logins based on the county's public IP address(es)?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Authorized users, through the NextGen SCP user interface, can limit access to the system based on a user's IP address, as shown in the following image.

Restricting Access by IP Address

The screenshot shows a configuration page titled "Restricting Access by IP Address". It contains two sections: "Access Time" and "Access Location".

- Access Time:** This section has two radio button options: "Anytime" (which is selected, indicated by a green dot) and "Limited (specify Schedule)".
- Access Location:** This section has two radio button options: "Anywhere" (which is selected, indicated by a green dot) and "Limited (specify IP addresses)".

- d. Provide a security plan.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

### Physical Security Measures for Securus Facilities

In terms of physical security measures to control access to the Securus network facilities, data centers, and corporate sites, security personnel are on premise 24x7x365. Security cameras (CCTV) are in use; cardkey reader (electronic badge)

access is required for entry. Multiple checks ensure data center physical security, including guarded, photo-verified check-in; dual-door authentication (card and biometric). All persons having a business need to access company premises must carry identification badges at all times. Man traps (interlocking door controllers) are located at each entry and exit point in the data center.

All visitors, customers, contractors, and repair personnel must gain access from the security officer on duty. Customers, contractors, repair personnel, maintenance personnel, and non-local employees can access buildings and critical areas only with an escort. Vendors may access buildings and critical areas only during working hours and also require an escort. IDF rooms and server rooms require special badge access.

## Security Defense Strategy and Network Protection

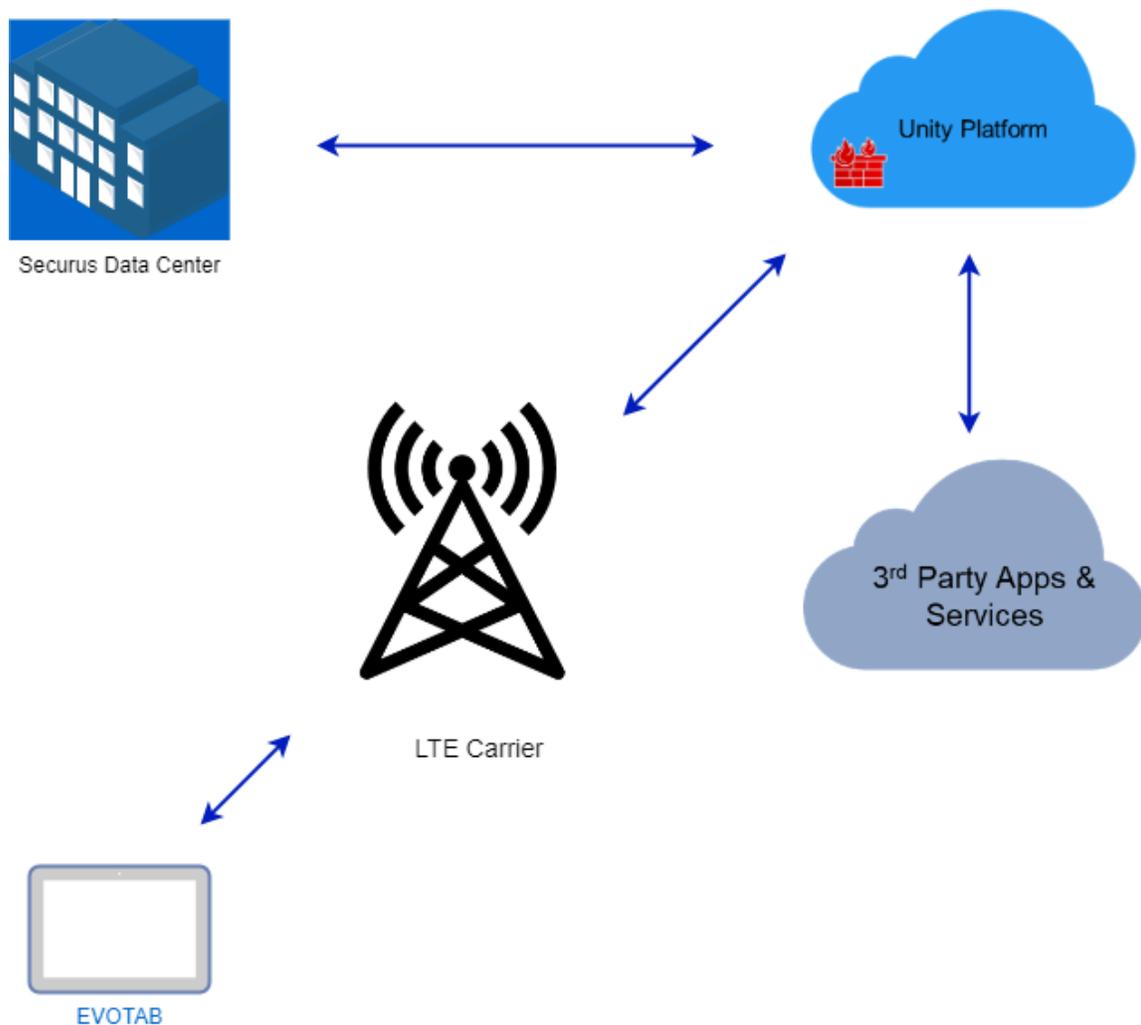
Securus uses a defense-in-depth security strategy, architecting the network into security zones at appropriate levels, while protecting and segregating users, applications, and databases. We enact strong access control policies that restrict access-based roles and policies to data and systems. A unique identification is assigned to each person for accountability for all actions while using our systems. Securus enforces strong, complex passwords and multi-factor authentication (MFA) across our enterprise networks and systems.

Securus deploys and manages next-generation firewalls configured with highly-restrictive access control lists (ACLs) that limit network traffic to pre-approved systems, and prevent Internet access per correctional industry guidelines and standards. The network is monitored for anomalous traffic 24x7x365. Collaboration between Securus' in-house cybersecurity incident response team (CIRT) and managed security service providers (MSSPs) provide monitoring and detection and response capabilities at all times.

Intrusion Detection / Prevention Systems (IDS/IPS) are installed at key points along the network, for monitoring and alerting 24x7x365. Egress/Ingress filtering is performed through next-generation firewalls, to deny communications with insecure/unused/unauthorized protocols, ports and services, and to limit access only to necessary and trusted IP address ranges. The threat signatures on the IDS/IPS devices are updated constantly, ensuring they are up-to-date with the latest threats. Notifications from various monitoring technologies on the network are investigated by the Securus Security Operations Center/Cyber Incident Response Team (SOC/CIRT). Our response process includes identification, containment, eradication, recovery, and post-incident reviews activities. Incidents or security breaches, should they occur, are handled in accordance with our data breach policy and incident response plan.

## EVOTAB Security

EVOTAB is the corrections industry's first Google-certified tablet with cellular connection capability. The EVOTAB utilizes a secure VPN connection over the carrier's LTE network to connect to the Unity Platform and through it to the various Unity service offerings. The EVOTAB is managed by a Google certified Enterprise Mobility Management (EMM) tool that provides control over the tablet.



Both the EVOTAB hardware and software have industry-best security practices. Internet access is restricted, ensuring users can only visit authorized websites and cannot surf the internet or communicate through unauthorized channels with anyone

outside of the facility. All of the infrastructure including the EVOTAB itself are monitored 24 x 7 to detect attempts to circumvent security controls. Customers are notified of any unusual activity within standard SLA times. Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.

### **Tablet Hardware and Firmware**

Securus EVOTAB is a corrections-grade hardened tablet that runs an android enterprise certified firmware created by our hardware partner. The features available in the firmware are controlled by the EMM also created by our hardware partner. The following security measures have been taken to harden the firmware on these tablets:

- The EMM controls what applications are installed and available to the user.
- Configuration settings have been restricted to only necessary settings.
- Authorized applications are pushed to the tablets through the EMM, thus preventing Incarcerated Individuals from installing or un-installing apps.
- Tablet network access is controlled by industry leading firewalls.
- Tablets are also prevented from accessing third-party app stores.

### **LTE Access**

The EVOTAB is pre-configured at the warehouse to connect to an authorized LTE carrier and is prevented from connecting to any other network through the security controls enforced via the EMM.

### **Data Centers**

Securus maintains a presence in multiple data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches, and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches.

**Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.**

### Security Layer 1

#### Tablet Firmware

Securus EVOTAB Tablets run a custom-developed proprietary firmware to harden their security and prevent any access to unauthorized content by the Inmates. The customized firmware does not have any of the common apps that are found on consumer-grade tablets.

The following security measures have been taken to harden the firmware on these tablets:

- Browser, contacts, calendar, native phone, and messaging clients have been removed.
- The option to change configuration settings has been removed.
- Near-field Communication (NFC) and Bluetooth have been disabled, except for Wi-Fi (where applicable/approved).
- Authorized applications are pushed to the tablets through Securus' app state management process, thus preventing Inmates from installing or un-installing apps.
- Tablets are prevented from accessing the public internet directly.
- Tablets are prevented from accessing third-party app stores.

#### Wi-Fi Access

The firmware only allows the tablets to connect to a Securus-provided network using a unique SSID (Service Set Identifier) for Wi-Fi. Security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses wireless access points (WAPs) that are customized only to broadcast the SSID to supported EVOTAB Tablets.

## Security Layer 2

### Securus Local Platform

All the WAPs are connected to a Securus Local Platform (SLP) running Securus' custom- developed proprietary software. These SLPs have components that inspect all the network packets and provide firewall, transparent proxy, DHCP, DNS, and routing services for the tablets.

The SLP is essential to all tablet functions and is configured to govern what the tablets can access. The tablet cannot receive any content from a network that the SLP has not been configured to provide. The SLP inspects all tablets' traffic and ensures that access is granted only to authorized content.

Although a tablet can connect to the Wi-Fi network, it cannot obtain an IP (internet protocol) address unless it is recognized as an authorized device by the SLP. If a tablet is not known by the SLP, it will *not* be granted access to the wireless network and will be rendered useless for applications that require network connectivity.

The SLP at the facility premise is connected to Securus' data center over an Internet Protocol Security Virtual Private Network (IPsec VPN) tunnel. The IPsec VPN service provides secure IP communications by authenticating and encrypting each IP packet of a communication session.

## Security Layer 3

### Data Centers

Securus maintains a presence in three data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches, and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches.

## 6. Network Compatibility

### a. What is the minimum actual network throughput and latency?

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As with all Securus services, all solutions are supported out of our carrier class data centers located in Dallas, Texas; Atlanta, Georgia; and Miami, Florida. All client information, recordings, and applications are stored within these secure facilities.

Securus provides all required network connectivity and does not require your facility to provide any network infrastructure. As a point of policy, Securus does not use client-provided network infrastructure. By providing our own network, we can monitor the network through our Network Operations Center (NOC) and can provide quick network resolution through our Technical Support Center (TSC) 24x7x365 without contacting or coordinating with our clients or client network providers.

Also, we provide and maintain all of the on-site network connectivity equipment through our nationally disbursed certified technicians that carry all necessary replacement components.

To support the EVOTAB Tablet application, Securus specifically designed a wired and wireless network that ensures a safe and secure environment. As we transition to EVOTAB we recommend using our **secure LTE solution**. This provides SIM based security, in an always on VPN that is always directly whitelisted with the carrier network to only route traffic to our data centers, allowing us to maintain full control of the connectivity and any breakout.

Our calling platform supports more than 1,700 sites and handles approximately 25,000 concurrent calls during peak calling times. The network is engineered to support more than 45,000 concurrent calls. The **number of telephones attached to our NextGen SCP is unlimited**, and it is our policy to have 30% more capacity available than peak volume level.

- b. Describe how the system will work in an environment of intermittent mobile computer connectivity.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus uses a matrix that provides the optimal network speeds and bandwidth for the services being used by Sedgwick County. On this network, whitelisting only allows for a very limited number of sites to be reached, of which are related to Securus services. In addition, security measures keep only ad hoc devices on the network.

The majority of our other sites use an ISP to have internet connectivity for agency staff and others visiting the site.

- c. What is the slowest wired network connection speed that is required to support the system?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus provides network speeds needed to support the system, so this questions in not applicable.

- d. What is the slowest wireless network connection speed that is required to support the system?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus provides network speeds needed to support the system, so this questions in not applicable.

## 7. System Software Application and Utilities

- a. Provide the name, company, and release level of any additional third-party software required to support the proposed solution.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus does not require any 3rd party software to support the proposed solution.

NextGen SCP is a centralized, digital network that is accessed via the web by navigating to <https://ngscp.securustech.net> in the supported browser, Chrome.

## 8. System Software Requirements

- a. Define if you host databases on SQL Servers. Can shared SQL servers be used?

---

**Securus Technologies**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

All of Sedgwick’s data is stored at our data centers, and all data retrieval for Sedgwick is through our NextGen SCP User Interface. Securus does not host anything locally at the facility for our calling platform, tablets or video visitations.

- b. Which versions of SQL server is the system compatible with? Include version number and edition. SQL server versions must not be end of life or near end of life.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus offers our NextGen SCP User Interface, which is internet driven, which does not require an SQL server at the Sedgwick facilities.

- c. What is the number of required cores and what are the memory requirements on the SQL server?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus offers our NextGen SCP User Interface, which is internet driven, which does not require an SQL server at the Sedgwick facilities.

- d. What administrative rights will you need during set-up and once the system is live?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus maintains all administrative rights, allowing Sedgwick access to all requested data.

## 9. System Backup

- a. Describe the recommended approach for system backup.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We use a digital backup system to minimize the cost of ownership related to data cartridges and tape. By incorporating a mix of daily, weekly, monthly, and quarterly backups, Sedgwick County will have a complete history of your CDRs from various points in time.

Communication recordings are available for playback immediately. As an additional layer of protection, we replicate communication recordings between the Dallas and Atlanta data centers.

b. How will the proposer's recommended backup process affect live operation?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Daily live operations are not affected by Securus' proven backup process.

c. Are all system functions (inquiry and update) available during backup? If not, explain the level of availability of system functions during backup and approximate time to perform backup.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Yes, all system functions will be immediately available during system backups. There is no interruption of live operations.

d. Will the recommended approach enable full backup of the system?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

e. Can the full backup be performed unattended?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Yes, full backups can be performed unattended and on a schedule.

f. Can full backup be scheduled to occur automatically?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Yes, full backups can be performed automatically on a schedule.

g. Can the system perform incremental backup (i.e. only data/files updated since last backup)?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We use a digital backup system to minimize the cost of ownership related to data cartridges and tape. By incorporating a mix of daily, weekly, monthly, and quarterly backups, Sedgwick County will have a complete history of your CDRs from various points in time.

Communication recordings are available for playback immediately. As an additional layer of protection, we replicate communication recordings between the Dallas and Atlanta data centers.

h. How long (estimated) will it take and what steps are involved to restore from a backup?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Our Business Continuity Plan (BCP) documents how all operating configurations and critical data is stored on backups that are archived at a secure remote location to provide quick recovery in the event of downtime or data loss. The document provides high-level guidance to the support staff responsible for the continuance of operations.

Since the data from calls, video sessions and messaging are all stored in our data centers for your immediate access via internet, there is minimal data that would need to be restored to local memory from a backup. This can be done in a matter of minutes depending on the size of the backup.

## 10. Database

### a. What encryption options do you utilize?

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Protecting your data:** Securus developed a strong corporate Information Security Governance and Cyber-Security framework using the NIST guidelines, including 800-53 current version. Applications transmitting data across public networks support TLS 1.2 with AES-256 bit encryption. Sensitive data is encrypted both at rest and in motion. Securus provides support for TLS encryption at the application network layer. All web sessions and services are conducted via HTTPS using AES 256-bit encryption. Securus uses a gold-class vendor-provided certificate service for external and internal SSL connections.

The NextGen SCP user interface encrypts and decrypts user page requests, as well as the pages that are returned by the web server. Access to Securus server information is done through HTTPS—HTTP application layering with Transport Layer Security (TLS) as a sub-layer. The use of HTTPS protects against eavesdropping and man-in-the-middle attacks (events where attacker secretly relays, and possibly alters, the communication between two parties who believe they are directly communicating with each other).

**CJIS-compliant access:** Securus uses an industry-recognized leader to provide remote access to Securus systems within state networks. This remote access system provides secure, encrypted, CJIS-compliant access to Securus systems. Securus also uses a state-of-the-art Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) to monitor and protect our network boundaries. Securus infrastructure servers and all workstations require anti-virus protection and receive regularly scheduled security patches and updates

For your team, NextGen SCP can enforce strong password policies for individual with minimum password length, 30-/60-/90-day password expirations, case sensitivity requiring upper- and lower-case letters, and special characters (@, #, \$, etc.).

### b. Are replication servers required for backups?

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional

layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

- c. The product should allow read only access to the system database or replicated database to facilitate the ability to bring data into SAP BI for ERP. In addition, the preference would also be to have access to the system's data dictionary/schema. This may not be required.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

This is not applicable to Securus' system.

## 11. Data Conversion Plan

In this subsection, please provide a Conversion Plan and approach – Data from current systems must be converted to the new system. The Data Conversion Plan must describe the strategy, approach, processes and reference the appropriate specifications to convert data from the county's current systems to the new system.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Since Securus is the incumbent at Sedgwick County Detention Facility, there is no need for any data to be converted.

## 12. Deployment/Implementation

In this subsection the Vendor must provide a detailed Deployment and Implementation plan which documents the activities that must be performed to deploy the application to the production environment and implement within the county. The plan must detail elements related to the critical activities that need to be performed prior to launch. The plan must contain the detailed installation procedures and consider the inter-application dependencies. The plan must include the step-by-step activities leading up to deployment as well as the post- deployment activities related to reporting and clean-up. Additionally, the plan must address the

roles and responsibilities, Go/No-Go criteria and decision date, required resources, assumptions, and risks related to implementation and Go-live.

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

As the incumbent provider of services for Sedgwick County, **our implementation process will be minimal and will not disrupt your current services and operations.** We'll transition you to SVC on NextGen SCP and replace/upgrade your tablets for an **enhanced experience by both inmates and your officers.**

For any implementation and installation work that may be required, we follow a tested process—the same process we used when we originally installed our service and products at Sedgwick County. The following pages outline that standard process. For any activities that aren't necessary due to our existing integrations and implementation, we'll proceed to the next step—providing you with a **faster, more seamless and efficient implementation experience.**

## **Standard Implementation Process**

The Securus Implementation Team delivers a quality installation and no mess. Our post-implementation customer surveys demonstrate that agencies appreciate our approach and experience, including these benefits.

- **Clean install** and greater reliability
- **Attention to detail** upfront and less maintenance later
- **Standard install** and streamlined troubleshooting

**Securus services are successfully installed at** approximately 1,800 **corrections facilities of all sizes** using our five-phased Implementation Plan. We bring this experience to your project and strive for a seamless installation and transition of service at Sedgwick County facilities. During the implementation and testing process, **we minimize the** Sedgwick County **administrative burden**--your team and resources remain focused on their primary responsibilities while we manage an efficient implementation.

The Securus Implementation Plan for the Sedgwick County project includes a turnkey installation of all equipment, facilities, and connectivity that is scheduled to go live within 60 days of contract execution. Your requirements are included in the plan along with built in flexibility to address challenges that may occur along the way. Downtime during transition is limited and the needs of your population and their families will be addressed through support and training.

## SECURUS — A REVIEW ON OUR SERVICE

“The Securus Installation Team is the most professional group of people that I have ever had the pleasure of working with on this type of project. Their attention to detail and dedication to customer satisfaction allowed them to complete a statewide, multi-location installation well under the projected completion date with virtually no unforeseen problems. I would love to work with them on another project.”

-- Karl Prince, IT Manager, Louisiana DOC

## Implementation Project Phases

The Securus Implementation Plan has five project phases with quality control checkpoints at key stages throughout the project. The quality control checkpoints are part of the Securus Six Sigma quality measurement that is used to identify and remove the causes of errors and minimize variability in the installation process. Each installation follows a defined sequence of steps with quantifiable targets—financial, time, or any other measure that is important to you.

### Phase 1: Project Initiation

After contract award, the Securus Project Team meets with Sedgwick County onsite for introductions, scope and timetable review, site survey confirmation, project communication and meeting plan, and project kick-off.

### Phase 2: Project Planning

The Securus Project Team coordinates material, human resources required for the project, travel, facility access, deliveries, and customer training. Securus works directly with all interstate, intrastate, and local exchange carriers (LECs) to coordinate the installation of network services and equipment required for the project.

### Phase 3: Project Execution

The Securus Project Team will provide regular progress reports to Sedgwick County and, at your option, hold a weekly meeting with Sedgwick County. Securus Implementation Technicians travel to each location and complete pre-installation activities including wiring, hardware staging, and telecom test/turn-up activities that can be done in advance to reduce the time and complexity of the actual cut-over. The Securus Project Team coordinates implementation activities with Sedgwick County and the current service provider to ensure a seamless transition of service. If a service

interruption is required, the activity will be coordinated with the Sedgwick County team at least five business days in advance. Most project activity will occur during normal business hours; however, Securus can accommodate work late-night, overnight, and during lockdown.

Securus performs a thorough inspection of the installation and resolves issues. Securus Installation Technicians perform a walk-through with the Sedgwick County team to review all installation documentation and checklists. The Securus Project Team hosts a customer acceptance review meeting with the Sedgwick County team after finalizing the implementation at each location. In addition, onsite training, and web-based training activities (if applicable) occur during this phase of the project.

- **Quality Control Checkpoint 1**  
Customer Provisioning prepares the Securus systems to support the Sedgwick County installation at required levels and configures necessary applications and calling features.
- **Quality Control Checkpoint 2**  
Customer Pre-Installation reviews onsite equipment inventory, equipment location, electrical, network, telecommunication, and telephone/ terminal installation standards to confirm Securus standards are met or exceeded.

#### Phase 4: Project Monitoring/Controlling

Outstanding items are resolved, and the Securus Team conducts daily diagnostic checks and monitoring. Sedgwick County confirms project requirements were achieved.

- **Quality Control Checkpoint 3**  
Equipment Testing / Functional Validation tests the system functionality while online to confirm all system options are configured to meet Sedgwick County specifications and requirements.

#### Phase 5: Project Closure

The Securus Project Team and Sedgwick County review the project. Once Sedgwick County team delivers final acceptance, the Securus Project Team will seamlessly transition support responsibilities to your Securus Account Manager. After Project Closure, the Securus Account Management Team and Technical Support Teams are available 24x7x365. Securus will provide Sedgwick County with phone and email contact information and escalation procedures for all ongoing maintenance and support needs.

- **Quality Control Checkpoint 4**

Customer Acceptance involves a meeting for Sedgwick County review of all quality control documents, equipment inventory records, and network diagrams. Resolution of any outstanding deliverables or service issues occurs before completing the Customer Acceptance checkpoint.

## Transition Period with Minimum Service Disruptions

By installing all ITS equipment and circuits prior to the cutover date—usually one to two weeks in advance of the cutover date—this allows for all systems, circuits, etc., to be fully tested. By testing prior to cutover, there is no risk of service interruptions due to the change-over to the new system. Our team has used this process with much success throughout their many multiple site accounts in the US & Canada.

We'll install and test all necessary equipment and circuits at each site prior to the actual cutover date. After the system is installed, it will be running on our circuits and will not have any impact on the system. There will be no interruption of service at that time. On the cutover date, the hardware will be unplugged from the existing system and reconnected to our system. There will not be any interruption of service. The cutover may be conducted during the time the facility has all phones/hardware off, i.e., a count time, prior to the hardware coming on at the beginning of the day, or after the equipment goes off for the day. This minimizes any downtime for the facilities.

We will coordinate any removal of the existing hardware in all of the Sedgwick County facilities. After all instruments have been replaced, the new system will be flash-cut from your existing vendor to Securus during low-use time periods. Typically, the time required for instrument change-out is less than 10 minutes per phone. All onsite work will be performed in accordance with Sedgwick County policies and at your convenience.

We do support late-night transitions to our proposed technology to further mitigate downtime. Using this approach, our team installs and tests all systems, and then after the majority of the population has been locked down for the evening, we begin the system cut-over, starting with the booking and intake areas, then moving to bring the other areas online, based on the County's established priority. The system will be fully transitioned when the inmates begin their day.

Our teams avoid disruption of services and creating undue work for Sedgwick County staff.

### Testing

Each system is placed under 'stress-testing' for seven days before it leaves the production facility. This testing procedure simulates that all ports on the system are in constant use 24 hours straight, for 7 days. The system is again tested onsite to ensure

total functionality. Test communications are placed from each station to each trunk. The network integration is validated through a battery of tests that include frame testing and file transmission.

## Training

We provide ongoing product training on all NextGen SCP features deployed at the County, at no cost. We want your staff to use the tools we provide, and training is essential to the adoption process. Experienced Securus employees conduct all training through online, instructor-led classes or on-site, one-on-one and classroom training sessions at no cost to you. We deliver standard training using both hands-on experience with your data and instructor demonstrations to ensure each trainee understands all concepts.

Our training programs enable facility staff to use all features the first day of installation. Because NextGen SCP is web-based, after a two- to three-hour training session, most users find it easy to use the system immediately.

In addition to standard training, we'll work with you to customize your training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions, such as, creative investigations, well-organized live call monitoring, and efficient system administration. Training for product upgrades, new facility staff, or a general refresher course is offered through online instructor-led courses available twice a month throughout the year—ongoing training ensures your staff understands current and new NextGen SCP features.

## County Staffing Responsibilities

### Degree of Involvement from Sedgwick County

We limit the administrative burden that can occur during a transition of service providers. We have the experience of installing our services in approximately 1,800 customer locations—more experience than any of our competitors. This level of experience ensures that we do not waste any time. Our teams arrive at your facilities ready to get the job done.

At the beginning of the project, the Securus Project and Implementation Teams will meet with the County onsite at a County location, or virtually if Sedgwick County prefers. These meetings allow us to introduce the project members and review the project plan and timetables with the Sedgwick County Team in person and ensure a successful kick-off to our project.

Our Project Managers will work with the County Team to coordinate equipment deliveries and facility access. When our technicians arrive onsite, they may require escorts to the equipment locations. The majority of our project activity will occur during normal business hours. Again, we can accommodate late-night/overnight cut-over

activities. Some of our customers choose this method to eliminate service interruptions and reduce interaction with inmates.

## Post-Implementation Communications

For the duration of the contract, Securus' Client Services Manager will be the primary point of contact for ongoing maintenance and support needs.

Securus' Field Services Manager and Account Manager are accessible by telephone and email 24 x 7x 365.

Sedgwick County is provided with our escalation procedure and appropriate contact information, which may include telephone numbers, email addresses, fax numbers, or other requested information.

Sedgwick County facility personnel will be provided with Securus' toll free Technical Support number and email address. Our Technical Support number is answered 24 x 7x 365 by a Securus Technical Support Representative.

Your Account Manager will provide the County with the required or requested reports based on information in system databases, such as communication detail reports, traffic statistics, revenue, system usage, and performance reports. If desired, we will provide periodic system service reports to demonstrate system uptime. Based on the County's preference, service reports can be provided via mail, email, or Internet download from our Secure FTP Report Server.

## Quarterly Performance Reviews

Securus has assigned a dedicated account management team, which includes not only the sales and support staff, but also the County's assigned Account Manager who will monitor the ongoing service and maintenance request and will conduct regularly scheduled site visits to ensure that you are receiving the highest level of customer service. In addition to these site visits, we offer quarterly Operational Reviews in which your Account Manager will meet with Sedgwick County staff and discuss operational performance, successes, and opportunities for improvement. We use the information from these meetings to improve our service delivery platform. This approach allows us to consistently perform at Net Promoter Scores that are among the highest recorded by any business in any industry.

## Minimizing the Transition Impact to Inmates, Staff, and Friends and Families

We will address the needs of inmates, staff, and friends and families to minimize the impact of transition. Changing from the County's incumbent service to Securus' service is not difficult, and we are prepared to support all aspects of the transition to minimize impact.

Our experience with the security and operations of inmate facilities will expedite the tasks of site surveys and new equipment installation. We plan on-site activities to minimize disruption.

We will provide an extensive and comprehensive training program both initially and ongoing for Administrative and Investigative personnel.

Downtime of service to inmates will be minimal. Securus and the County will develop a plan of installation times and dates that reduces the downtime for the inmate population at all County locations.

Prior to the transition to a new system, we will provide a calling campaign to the phone numbers that are in the County database informing them of the new system and how to use the services going forward. A Securus phone number and website will be provided to assist them in the change. Securus' Customer Service Center will also be instrumental in the smooth transition of services.

**At a minimum, the deliverable must contain the following:**

**a. Deployment strategy and approach**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *9. Deployment/Implementation*, at the beginning of this subsection and the attached project plan under Attachment A.

**b. Software installation procedures**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Since NextGen SCP is a web-based platform, there is no software installation required. All tablets and kiosks come with software pre-installed.

**c. Deployment/Conversion implementation detailed plan**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *9. Deployment/Implementation*, at the beginning of this subsection and the attached project plan under Attachment A.

d. Post deployment activities

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under 9. *Deployment/Implementation*, at the beginning of this subsection and the attached project plan under Attachment A.

e. Proposed scope, approach, schedule and team

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under 9. *Deployment/Implementation*, at the beginning of this subsection and the attached project plan under Attachment A.

f. Implementation phase entry and exit criteria

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under 9. *Deployment/Implementation*, at the beginning of this subsection and the attached project plan under Attachment A.

g. Implementation readiness approach (go/no-go criteria and checklist)

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Refer to Quality Control Checkpoints in response above as go/no-go criteria.

Please reference Attachment B for Sample Implementation Checklist

## PROJECT MANAGEMENT

Include the following information in this subsection: Describe the Vendor's approach to managing the implementation of the proposed system, addressing at a minimum the following components of project management:

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**We do the work:** Our Implementation Plan limits the burden for Sedgwick County. During the kick-off meeting you will designate a person or team to be the point of contact for Securus. Responsibilities will be limited to the following:

- Scheduling – Our Team will work with your designated point of contact to streamline and schedule site surveys, equipment deliveries, technician work,

and training. The Securus project manager will monitor scheduled completion dates.

- Status Report Review – Throughout the project, our Project Management and Implementations Teams provides weekly progress reports with updates on active, completed, and pending installation activities.
- Status Meetings – We recommend a weekly meeting with a prepared agenda distributed in advance to make it easy for Sedgwick County to ask questions and discuss issues.
- Site Escort Coordination – Sedgwick County will provide required escorts as needed. Most work is completed during business hours but we can accommodate after-hours work if preferred. Our technicians perform the site surveys, equipment installation, and any disposal required.
- Training – Sedgwick County will provide onsite space for training. We'll provide hands-on training to the Sedgwick County team.
- Final Walk-Thru and Approval – Securus will join Sedgwick County in site and checklist review as the project transitions to active status. This may occur in phases throughout the project.

**We make it easy:** The Securus Team provides the support you need:

- Implementation Team – We take care of all project management.
- Sales Engineers Team – We want you to have the advantage of our extensive industry experience, knowledge of best practices, and ability to work with you for the best solutions. Our Sales Engineers work hard to get maximum benefit to Sedgwick County.
- Integration Team – Securus designs, develops, tests, and implements all custom integrations for the Sedgwick County project. Our technology has the flexibility to work with facility-owned systems, JMS, OMS, commissary, banking, and kiosk vendors. Securus will fully cooperate with your facility and your vendors to automate systems. The most common technologies we use include SOAP Web Services, HTTPS, FTP push or pull of files in any text format, JSON, XML-RPC, and TCP Sockets. We currently integrate with more than 110 different vendors worldwide and more than 60 independent, facility-owned systems, and shared databases.
- Account Management Team – Sedgwick County will be assigned a Securus Account Manager who proactively manages the day-to-day needs of your facilities, monitoring systems and product usage, quarterly operational reviews, site visits, and additional product training.
- Technical Support Center and Field Services Team – Securus provides ongoing maintenance and support for all products and services. Sedgwick

County will have contact information and escalation procedures so you get quick response and issue resolution.

- Regulatory Team – Securus stays current on the continuously changing rules and regulations relating to the services and products we provide locally and nationally. We provide updates and work with you if changes are needed for ongoing compliance throughout the term of our contract.

**a. Project communications**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *B. Project Management*, at the beginning of this subsection.

**b. Schedule management**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *B. Project Management*, at the beginning of this subsection.

**c. Issue management**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *B. Project Management*, at the beginning of this subsection.

**d. Scope management**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *B. Project Management*, at the beginning of this subsection.

**e. Risk management**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to our response under *B. Project Management*, at the beginning of this subsection.

Risk management has executive level visibility and support.

## f. Quality assurance

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus will work with the Sedgwick County to reach mutual agreements on implementation plans as well as any subsequent changes. Our experience implementing similar programs can be used to Sedgwick County's advantage to provide an expedited implementation and roll-out.

As the incumbent provider of services for Sedgwick County, **our implementation process will be minimal and will not disrupt your current services and operations.** We'll transition you to SVC on NextGen SCP and replace/upgrade your tablets for an **enhanced experience by both inmates and your officers.**

For any implementation and installation work that may be required, we follow a tested process—the same process we used when we originally installed our service and products at Sedgwick County. The following pages outline that standard process. For any activities that aren't necessary due to our existing integrations and implementation, we'll proceed to the next step—providing you with a **faster, more seamless and efficient implementation experience.**

## Standard Implementation

The Securus Implementation Team delivers a quality installation and no mess. Our post-implementation customer surveys demonstrate that agencies appreciate our approach and experience, including these benefits.

- **Clean install** and greater reliability
- **Attention to detail** upfront and less maintenance later
- **Standard install** and streamlined troubleshooting

**Securus services are successfully installed at** approximately 1,800 **corrections facilities of all sizes** using our five-phased Implementation Plan. We bring this experience to your project and strive for a seamless installation and transition of service at Sedgwick County facilities. During the implementation and testing process, **we minimize the** Sedgwick County **administrative burden**--your team and resources remain focused on their primary responsibilities while we manage an efficient implementation.

The Securus Implementation Plan for the Sedgwick County project includes a turnkey installation of all equipment, facilities, and connectivity that is scheduled to go live within 60 days of contract execution. Your requirements are included in

the plan along with built in flexibility to address challenges that may occur along the way. Downtime during transition is limited and the needs of your population and their families will be addressed through support and training.

#### SECURUS — A REVIEW ON OUR SERVICE

“The Securus Installation Team is the most professional group of people that I have ever had the pleasure of working with on this type of project. Their attention to detail and dedication to customer satisfaction allowed them to complete a statewide, multi-location installation well under the projected completion date with virtually no unforeseen problems. I would love to work with them on another project.”

-- Karl Prince, IT Manager, Louisiana DOC

## Implementation Project Phases

The Securus Implementation Plan has five project phases with quality control checkpoints at key stages throughout the project. The quality control checkpoints are part of the Securus Six Sigma quality measurement that is used to identify and remove the causes of errors and minimize variability in the installation process. Each installation follows a defined sequence of steps with quantifiable targets— financial, time, or any other measure that is important to you.

### Phase 1: Project Initiation

After contract award, the Securus Project Team meets with Sedgwick County onsite for introductions, scope and timetable review, site survey confirmation, project communication and meeting plan, and project kick-off.

### Phase 2: Project Planning

The Securus Project Team coordinates material, human resources required for the project, travel, facility access, deliveries, and customer training. Securus works directly with all interstate, intrastate, and local exchange carriers (LECs) to coordinate the installation of network services and equipment required for the project.

### Phase 3: Project Execution

The Securus Project Team will provide regular progress reports to Sedgwick County and, at your option, hold a weekly meeting with Sedgwick County. Securus Implementation Technicians travel to each location and complete pre-installation activities including wiring, hardware staging, and telecom test/turn-up activities that can be done in advance to reduce the time and complexity of the actual cut-over. The Securus Project Team coordinates implementation activities with Sedgwick County and the current service provider to ensure a seamless transition of service. If a service interruption is required, the activity will be coordinated with the Sedgwick County team at least five business days in advance. Most project activity will occur during normal business hours; however, Securus can accommodate work late-night, overnight, and during lockdown.

Securus performs a thorough inspection of the installation and resolves issues. Securus Installation Technicians perform a walk-through with the Sedgwick County team to review all installation documentation and checklists. The Securus Project Team hosts a customer acceptance review meeting with the Sedgwick County team after finalizing the implementation at each location. In addition, onsite training, and web-based training activities (if applicable) occur during this phase of the project.

- **Quality Control Checkpoint 1**  
Customer Provisioning prepares the Securus systems to support the Sedgwick County installation at required levels and configures necessary applications and calling features.
- **Quality Control Checkpoint 2**  
Customer Pre-Installation reviews onsite equipment inventory, equipment location, electrical, network, telecommunication, and telephone/ terminal installation standards to confirm Securus standards are met or exceeded.

### Phase 4: Project Monitoring/Controlling

Outstanding items are resolved, and the Securus Team conducts daily diagnostic checks and monitoring. Sedgwick County confirms project requirements were achieved.

- **Quality Control Checkpoint 3**  
Equipment Testing / Functional Validation tests the system functionality while online to confirm all system options are configured to meet Sedgwick County specifications and requirements.

## Phase 5: Project Closure

The Securus Project Team and Sedgwick County review the project. Once Sedgwick County team delivers final acceptance, the Securus Project Team seamlessly will transition support responsibilities to your Securus Account Manager. After Project Closure, the Securus Account Management Team and Technical Support Teams are available 24x7x365. Securus will provide Sedgwick County with phone and email contact information and escalation procedures for all ongoing maintenance and support needs.

- **Quality Control Checkpoint 4**

Customer Acceptance involves a meeting for Sedgwick County review of all quality control documents, equipment inventory records, and network diagrams. Resolution of any outstanding deliverables or service issues occurs before completing the Customer Acceptance checkpoint.

## Transition Period with Minimum Service Disruptions

By installing all ITS equipment and circuits prior to the cutover date—usually one to two weeks in advance of the cutover date—this allows for all systems, circuits, etc., to be fully tested. By testing prior to cutover, there is no risk of service interruptions due to the change-over to the new system. Our team has used this process with much success throughout their many multiple site accounts in the US & Canada.

We'll install and test all necessary equipment and circuits at each site prior to the actual cutover date. After the system is installed, it will be running on our circuits and will not have any impact on the system. There will be no interruption of service at that time. On the cutover date, the hardware will be unplugged from the existing system and reconnected to our system. There will not be any interruption of service. The cutover may be conducted during the time the facility has all phones/hardware off, i.e., a count time, prior to the hardware coming on at the beginning of the day, or after the equipment goes off for the day. This minimizes any downtime for the facilities.

We will coordinate any removal of the existing hardware in all of the Sedgwick County facilities. After all instruments have been replaced, the new system will be flash-cut from your existing vendor to Securus during low-use time periods. Typically, the time required for instrument change-out is less than 10 minutes per phone. All onsite work will be performed in accordance with Sedgwick County policies and at your convenience.

We do support late-night transitions to our proposed technology to further mitigate downtime. Using this approach, our team installs and tests all systems, and then after the majority of the population has been locked down for the evening, we begin the system cut-over, starting with the booking and intake areas, then moving to bring the other areas online, based on the County's established priority. The system will be fully transitioned when the inmates begin their day.

Our teams avoid disruption of services and creating undue work for Sedgwick County staff.

### Testing

Each system is placed under 'stress-testing' for seven days before it leaves the production facility. This testing procedure simulates that all ports on the system are in constant use 24 hours straight, for 7 days. The system is again tested onsite to ensure total functionality. Test communications are placed from each station to each trunk. The network integration is validated through a battery of tests that include frame testing and file transmission.

### Training

We provide ongoing product training on all NextGen SCP features deployed at the County, at no cost. We want your staff to use the tools we provide, and training is essential to the adoption process. Experienced Securus employees conduct all training through online, instructor-led classes or on-site, one-on-one and classroom training sessions at no cost to you. We deliver standard training using both hands-on experience with your data and instructor demonstrations to ensure each trainee understands all concepts.

Our training programs enable facility staff to use all features the first day of installation. Because NextGen SCP is web-based, after a two- to three-hour training session, most users find it easy to use the system immediately.

In addition to standard training, we'll work with you to customize your training experience to meet the unique needs of your staff and facility. We offer separate classes focused on different agency functions, such as, creative investigations, well-organized live call monitoring, and efficient system administration. Training for product upgrades, new facility staff, or a general refresher course is offered through online instructor-led courses available twice a month throughout the year—ongoing training ensures your staff understands current and new NextGen SCP features.

## County Staffing Responsibilities

### Degree of Involvement from Sedgwick County

We limit the administrative burden that can occur during a transition of service providers. We have the experience of installing our services in approximately 1,800 customer locations—more experience than any of our competitors. This level of experience ensures that we do not waste any time. Our teams arrive at your facilities ready to get the job done.

At the beginning of the project, the Securus Project and Implementation Teams will meet with the County onsite at a County location, or virtually if Sedgwick County prefers. These meetings allow us to introduce the project members and review the project plan and timetables with the Sedgwick County Team in person and ensure a successful kick-off to our project.

Our Project Managers will work with the County Team to coordinate equipment deliveries and facility access. When our technicians arrive onsite, they may require escorts to the equipment locations. The majority of our project activity will occur during normal business hours. Again, we can accommodate late-night/overnight cut-over activities. Some of our customers choose this method to eliminate service interruptions and reduce interaction with inmates.

### Post-Implementation Communications

For the duration of the contract, Securus' Client Services Manager will be the primary point of contact for ongoing maintenance and support needs.

Securus' Field Services Manager and Account Manager are accessible by telephone and email 24 x 7x 365.

Sedgwick County is provided with our escalation procedure and appropriate contact information, which may include telephone numbers, email addresses, fax numbers, or other requested information.

Sedgwick County facility personnel will be provided with Securus' toll free Technical Support number and email address. Our Technical Support number is answered 24 x 7x 365 by a Securus Technical Support Representative.

Your Account Manager will provide the County with the required or requested reports based on information in system databases, such as communication detail reports, traffic statistics, revenue, system usage, and performance reports. If desired, we will provide periodic system service reports to demonstrate system uptime. Based on the County's preference, service reports can be provided via mail, email, or Internet download from our Secure FTP Report Server.

## Quarterly Performance Reviews

Securus has assigned a dedicated account management team, which includes not only the sales and support staff, but also the County's assigned Account Manager who will monitor the ongoing service and maintenance request and will conduct regularly scheduled site visits to ensure that you are receiving the highest level of customer service. In addition to these site visits, we offer quarterly Operational Reviews in which your Account Manager will meet with Sedgwick County staff and discuss operational performance, successes, and opportunities for improvement. We use the information from these meetings to improve our service delivery platform. This approach allows us to consistently perform at Net Promoter Scores that are among the highest recorded by any business in any industry.

## Minimizing the Transition Impact to Inmates, Staff, and Friends and Families

We will address the needs of inmates, staff, and friends and families to minimize the impact of transition. Changing from the County's incumbent service to Securus' service is not difficult, and we are prepared to support all aspects of the transition to minimize impact.

Our experience with the security and operations of inmate facilities will expedite the tasks of site surveys and new equipment installation. We plan on-site activities to minimize disruption.

We will provide an extensive and comprehensive training program both initially and ongoing for Administrative and Investigative personnel.

Downtime of service to inmates will be minimal. Securus and the County will develop a plan of installation times and dates that reduces the downtime for the inmate population at all County locations.

Prior to the transition to a new system, we will provide a calling campaign to the phone numbers that are in the County database informing them of the new system and how to use the services going forward. A Securus phone number and website will be provided to assist them in the change. Securus' Customer Service Center will also be instrumental in the smooth transition of services.

**Statement of Work that breaks down the system implementation by tasks and delineates Vendor and the county's responsibilities within each task. Tasks should include configuration, testing and interface development and deployment. Address project management services including creating and maintaining a detailed deployment plan, along with a detailed task list.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to the Quality Control Checkpoints in Implementation Plan above, specifically in Phases 3,4, and 5 .

**Realistic and readable implementation project schedule that starts at contract signing. The schedule should describe tasks to be performed by the county as well as by the Vendor.**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to Attachment A to view the detailed proposed Implementation Plan.

**How will the Vendor help the county or other external customers who interface with the county information systems identify potential changes in business processes because of changes in application software?**

### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus already has a well-established relationship with the county and external customers, who are familiar with our systems and processes. This familiarity allows us to efficiently communicate potential changes in business processes due to software updates, allowing smooth transition while minimizing disruptions.

Our training team is always available to provide ongoing training for Sedgwick County's staff.

Friends and family members are continuously educated on our products via Securus Online.

Your Account Manager, Michael Love, will continue to communicate with you on business process changes.

## **TRAINING**

**In this subsection the Vendor should describe how they would provide the following types of training programs, along with appropriate documentation:**

- a. A training program for county's project implementation team that includes the training necessary to understand the overall system architecture, interface configurations, data import/export capabilities, and workflow configuration options, etc.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has trained many of the county’s current project implementation team members, who are familiar with our system architecture, interface configurations, and workflows. This established knowledge base allows us to deliver streamlined, targeted training focused on any new updates or features. This allows us to provide a quick and efficient learning process for the team.

System functionally training is available to all Sedgwick County identified staff. Securus offers an extensive training program that entails phones, tablets and NextGen SCP applications. Additionally, on-line information is available 24/7.

**NextGen SCP Training Course Modules**

Securus is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. Training courses are offered in a user-friendly, task-oriented format to teach your staff what they need to know to do their jobs. We present courses in separate modules based on the types of duties officers tend to perform using the NextGen SCP inmate telephone system while focusing on the unique features of our applications.

The following table presents the standard NextGen SCP training course modules and associated learning objectives.

**NextGen Secure Communications Platform™  
Course Modules**

<b>Course Module</b>	<b>Objective</b>
<b>Overview and Navigation</b>	<ul style="list-style-type: none"><li>• Logging-in</li><li>• Navigating through the features</li><li>• Managing user password</li><li>• Managing user profile</li><li>• Manage system utility icons</li></ul>
<b>Dashboard</b>	<ul style="list-style-type: none"><li>• Review system announcements</li><li>• Manage widgets</li></ul>
<b>Monitor</b>	<ul style="list-style-type: none"><li>• Monitor live calls</li><li>• Forward Live Calls</li><li>• Add Notes to Live Calls</li></ul>
<b>Explore</b>	<ul style="list-style-type: none"><li>• Review INMATE Activity</li></ul>

	<ul style="list-style-type: none"> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> <li>• Review PAN Frequency</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>
<b>Manage</b>	<ul style="list-style-type: none"> <li>• INMATEs</li> <li>• INMATE PAN</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Control Call Settings</li> <li>• Create Security Roles</li> <li>• Manage Users</li> </ul>

### Tablet Course Modules

<b>Course Module</b>	<b>Objective</b>
<b>Command Staff</b>	<ul style="list-style-type: none"> <li>• Roles and Responsibilities</li> <li>• Procedural Best Practices Discussion</li> <li>• Tablet Usage and Distribution</li> <li>• Tablet Security</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Functionality of the INMATE Tablet</li> <li>• Communication Home, Accessing Forms</li> <li>• Filing a Form</li> <li>• Officer Controls</li> <li>• Distribution</li> <li>• Security</li> </ul>

**Telephone System  
Course Modules**

Course Module	Objective
<b>Overview and Navigation</b>	<ul style="list-style-type: none"> <li>• Logging-in</li> <li>• Navigating through the features</li> <li>• Managing user password</li> <li>• Managing user profile</li> <li>• Manage system utility icons</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Review system announcements</li> <li>• Manage widgets</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Monitor live calls</li> <li>• Forward Live Calls</li> <li>• Add Notes to Live Calls</li> </ul>
<b>Explore</b>	<ul style="list-style-type: none"> <li>• Review Inmate Activity</li> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> <li>• Review PAN Frequency</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>
<b>Manage</b>	<ul style="list-style-type: none"> <li>• Inmates</li> <li>• Inmate's PAN</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Control Call Settings</li> <li>• Create Security Roles</li> <li>• Manage Users</li> </ul>

### NextGen SCP with SVC Course Modules

Course Module	Objective
<b>Overview and Navigation</b>	<ul style="list-style-type: none"> <li>• Logging-in</li> <li>• Navigating through the features</li> <li>• Managing user password</li> <li>• Managing user profile</li> <li>• Manage system utility icons</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Review system announcements</li> <li>• Manage widgets</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Monitor live calls</li> <li>• Add Notes to Live Calls</li> </ul>
<b>Explore</b>	<ul style="list-style-type: none"> <li>• Review Inmate Activity</li> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>
<b>Manage</b>	<ul style="list-style-type: none"> <li>• Inmates</li> <li>• Inmate's PVL</li> <li>• Video Session Notification</li> <li>• Emergency Video Connect</li> <li>• Visits</li> <li>• Visitors</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Visitor Types</li> <li>• Visit Rules</li> <li>• Visit Schedules</li> <li>• Security Roles</li> <li>• Facility Portal</li> </ul>

	<ul style="list-style-type: none"> <li>• Install Video Chat</li> </ul>
--	--

**Self-Help Elements**

Online self-help is always available from a system Help menu in the product. Keyword searching offers immediate access to the information you are seeking or you can follow the table of contents for a full learning experience.

Officers can print one topic or the entire help system if a full user manual is preferred. This method of “print what you need when you need it” ensures all printed material is updated with the current released product.

**b. A training program for application administrators that includes the training necessary to configure, tailor, monitor, and administer the technical and functional aspects of system.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has trained Sedgwick County’s application administrators on how to configure, monitor, and manage the system. Their familiarity with the technical and functional aspects of the system allows us to focus on future training on any updates, new features, or advanced configurations. This allows us to provide a seamless and efficient training experience. As new administrators are introduced to the team, they will receive the support of their tenured teammates and from us.

Securus is committed to providing your staff with training that will maximize the potential of the features implemented at your facility. We are able to offer on-site and off-site training at no cost to Sedgwick County. Training courses are offered in a user-friendly, task-oriented format to teach your staff what they need to know to do their jobs. We present courses in separate modules based on the types of duties officers tend to perform using the NextGen SCP inmate telephone system while focusing on the unique features of our applications.

The following table presents the standard NextGen SCP training course modules and associated learning objectives.

**NextGen Secure Communications Platform™  
Course Modules**

Course Module	Objective
<b>Overview and Navigation</b>	<ul style="list-style-type: none"> <li>• Logging-in</li> <li>• Navigating through the features</li> <li>• Managing user password</li> </ul>

	<ul style="list-style-type: none"> <li>• Managing user profile</li> <li>• Manage system utility icons</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Review system announcements</li> <li>• Manage widgets</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Monitor live calls</li> <li>• Forward Live Calls</li> <li>• Add Notes to Live Calls</li> </ul>
<b>Explore</b>	<ul style="list-style-type: none"> <li>• Review INMATE Activity</li> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> <li>• Review PAN Frequency</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>
<b>Manage</b>	<ul style="list-style-type: none"> <li>• INMATEs</li> <li>• INMATE PAN</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Control Call Settings</li> <li>• Create Security Roles</li> <li>• Manage Users</li> </ul>

#### Tablet Course Modules

Course Module	Objective
<b>Command Staff</b>	<ul style="list-style-type: none"> <li>• Roles and Responsibilities</li> </ul>

	<ul style="list-style-type: none"> <li>• Procedural Best Practices Discussion</li> <li>• Tablet Usage and Distribution</li> <li>• Tablet Security</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Functionality of the INMATE Tablet</li> <li>• Communication Home, Accessing Forms</li> <li>• Filing a Form</li> <li>• Officer Controls</li> <li>• Distribution</li> <li>• Security</li> </ul>

**Telephone System  
Course Modules**

<b>Course Module</b>	<b>Objective</b>
<b>Overview and Navigation</b>	<ul style="list-style-type: none"> <li>• Logging-in</li> <li>• Navigating through the features</li> <li>• Managing user password</li> <li>• Managing user profile</li> <li>• Manage system utility icons</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Review system announcements</li> <li>• Manage widgets</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Monitor live calls</li> <li>• Forward Live Calls</li> <li>• Add Notes to Live Calls</li> </ul>
<b>Explore</b>	<ul style="list-style-type: none"> <li>• Review Inmate Activity</li> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> <li>• Review PAN Frequency</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>

<b>Manage</b>	<ul style="list-style-type: none"> <li>• Inmates</li> <li>• Inmate's PAN</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Control Call Settings</li> <li>• Create Security Roles</li> <li>• Manage Users</li> </ul>

### NextGen SCP with SVC Course Modules

Course Module	Objective
<b>Overview and Navigation</b>	<ul style="list-style-type: none"> <li>• Logging-in</li> <li>• Navigating through the features</li> <li>• Managing user password</li> <li>• Managing user profile</li> <li>• Manage system utility icons</li> </ul>
<b>Dashboard</b>	<ul style="list-style-type: none"> <li>• Review system announcements</li> <li>• Manage widgets</li> </ul>
<b>Monitor</b>	<ul style="list-style-type: none"> <li>• Monitor live calls</li> <li>• Add Notes to Live Calls</li> </ul>
<b>Explore</b>	<ul style="list-style-type: none"> <li>• Review Inmate Activity</li> <li>• Review Communication Records</li> <li>• Control Covert Alerts</li> <li>• Review System Logs</li> </ul>
<b>Investigate</b>	<ul style="list-style-type: none"> <li>• Open Investigator Pro</li> <li>• Open THREADS</li> <li>• Open ICER</li> <li>• Open WCS</li> </ul>
<b>Manage</b>	<ul style="list-style-type: none"> <li>• Inmates</li> <li>• Inmate's PVL</li> <li>• Video Session Notification</li> <li>• Emergency Video Connect</li> <li>• Visits</li> </ul>

	<ul style="list-style-type: none"> <li>• Visitors</li> <li>• eMessaging</li> </ul>
<b>Administration</b>	<ul style="list-style-type: none"> <li>• Control Facility and Sites</li> <li>• Control Phone Numbers</li> <li>• Visitor Types</li> <li>• Visit Rules</li> <li>• Visit Schedules</li> <li>• Security Roles</li> <li>• Facility Portal</li> <li>• Install Video Chat</li> </ul>

### Self-Help Elements

Online self-help is always available from a system Help menu in the product. Keyword searching offers immediate access to the information you are seeking or you can follow the table of contents for a full learning experience.

Officers can print one topic or the entire help system if a full user manual is preferred. This method of “print what you need when you need it” ensures all printed material is updated with the current released product.

- c. A training solution to support the training of end-users in the functionality of the various proposed system modules. To support the training of end users, the county envisions the use of a “train-the-trainer” approach. However, it is requested that all end users receive individual training.**

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

We have established a strong working relationship with Sedgwick County’s end-users, who are familiar with our system modules and functionality. This familiarity will allow us to streamline the “train-the-trainer” approach, while also efficiently providing individual training to all end-users, focusing on any new modules or features. This will minimize the time needed for training and enhance user adoption and proficiency.

Securus provides product training covering all features in the agreement at no cost to Sedgwick County. All training is conducted by experienced, certified trainers through onsite one-on-one and classroom training sessions or online instructor-led classes. Standard training is conducted using both hands-on experience with your data and using instructor demonstrations to ensure your personnel understand the processes and concepts presented. Securus’ training programs enable facility staff to use all features the first day of installation.

We offer separate classes focused on different agency functions using Securus' software. Trainers will conduct a needs analysis with your command staff to identify specific training requirements for each role at Sedgwick County.

In addition to standard on-site training, Securus offers separate training classes focused on different agency functions and products. Also, Securus offers online instructor-led courses available twice a month throughout the year for product upgrades, new facility staff, or general refreshers. *Securus' ongoing training ensures your staff always "stays on top" of new feature releases.*

### Initial Training

Securus' training programs generally take place during implementation, one to two weeks prior to go-live so facility staff can use all features the first day of installation.

The average class time is 2 ½ hours. Because our products are web-based and tablets are a familiar technology, after a two or three-hour training session, most facility staff can easily maneuver through the system's features. A typical class size for training is 5 to 20 people, although we can accommodate whatever size to meet the needs of Sedgwick County.

### Training Course Elements

Securus will provide your staff with training to maximize the potential of the features you selected. Training courses are in a user-friendly task-oriented format to teach your personnel what they need to know to do their job. Courses are often separated into modules based on the types of duties personnel tend to perform using the unique features of the product.

Please reference the response above for the modules included in our training.

#### d. Post implementation training.

##### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - CHANGED ANSWER**

Securus has an in-depth understanding of Sedgwick County's operations and end-user needs, which allows us to deliver highly targeted post-implementation training. Since users are already familiar with our systems, we can focus on new features and updates, allowing a smooth transition and quick adaptation with minimal disruption to daily operations.

Our training team is always available to provide ongoing training for Sedgwick County's staff. Online self-help is always available from a system Help menu in the product. Keyword searching offers immediate access to the information you are seeking or you can follow the table of contents for a full learning experience.

Officers can print one topic or the entire help system if a full user manual is preferred. This method of “print what you need when you need it” ensures all printed material is updated with the current released product.

Plus we are always here to help Sedgwick County with any post implementation training as well.

Friends and family members are continuously educated on our products via Securus Online.

**e. Multimedia presentations of training made available following actual training (e.g., PowerPoint presentations, videos, etc.).**

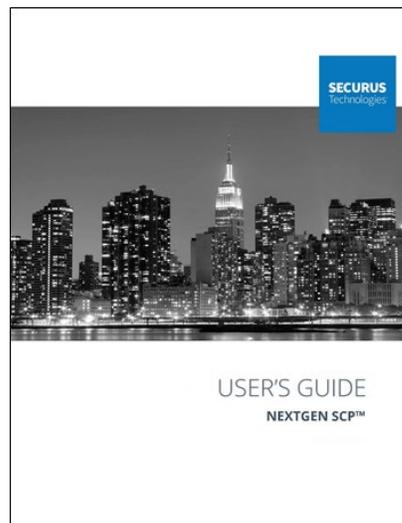
**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Online self-help is always available from a convenient Help menu accessible through NextGen SCP. PDF documents and videos are available for each of the sections that are available in trainings. Trainees use this PDF document to find quick answers to their questions about NextGen SCP. Keyword searching offers immediate access to the information or users can follow the table of contents for a full learning experience. Step-by-step instructions are designed to help the user complete tasks.

Officers can print one topic or the entire help system if a full user manual is preferred. Securus continuously upgrades and enhances NextGen SCP, so we recommend only printing the section needed to ensure all printed material is current.

The following figure illustrates the NextGen SCP online PDF document.

NextGen SCP Online Help



f. A training program that accounts for end users on shift work and may not be available during normal training hours.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Throughout the life of the contract, Sedgwick County staff can receive additional training at no cost to the County. This is especially useful if any of your facilities experience turn-over and new personnel must be trained, or for those users on shift work who aren't available during normal training hours.

Additional training can be conducted through a variety of methods, including:

- **On-site Classes** – Sedgwick County can contact your account manager to request additional on-site training. Your client manager will coordinate with the training department.
- **Webinars (Initial and Overview Training)** – Live webinars are conducted on a weekly basis by our trainers. These training sessions cover all aspects of the product being covered and go in depth into the product. These sessions are targeted at new facility staff who did not receive any training before. Securus records our webinars so that they can be sent electronically to Sedgwick County for training purposes if staff miss a session.
- **Webinars (Refresher Course and Updates)** - These online, instructor-led courses are also available twice a month throughout the year. These sessions focus on product upgrades or overviews for those who have already received in depth training but may need a refresher course.
- **Online task-based training videos** – These short videos can also be provided electronically and cover specific topic. The trainings can be accessed at any time.

## ARCHITECTURE AND IT STANDARDS

If web based, preferably written in HTML 5, not requiring Java, Reader, or Flash needs (vulnerable 3rd party apps) - if any, always the latest version.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

NextGen SCP is a web based system accessible by an internet browser connection and does not require a third party app to operate.

**Vendor should provide a list of client requirements.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

To fully use the NextGen SCP system and to benefit from all the available functions, Sedgwick County may choose to continue to participate in available training opportunities to include on-line refreshers. No other requirements are required.

**Vendor should indicate data requirements - data growth rate per year (database size, attachments, binaries, backup sizes, etc...). How does this impact costs and services?**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

Securus maintains all data requirements necessary to provide uninterrupted daily service to Sedgwick County. Securus continually monitors and plans for future growth that will continue to support the growth of Sedgwick County.

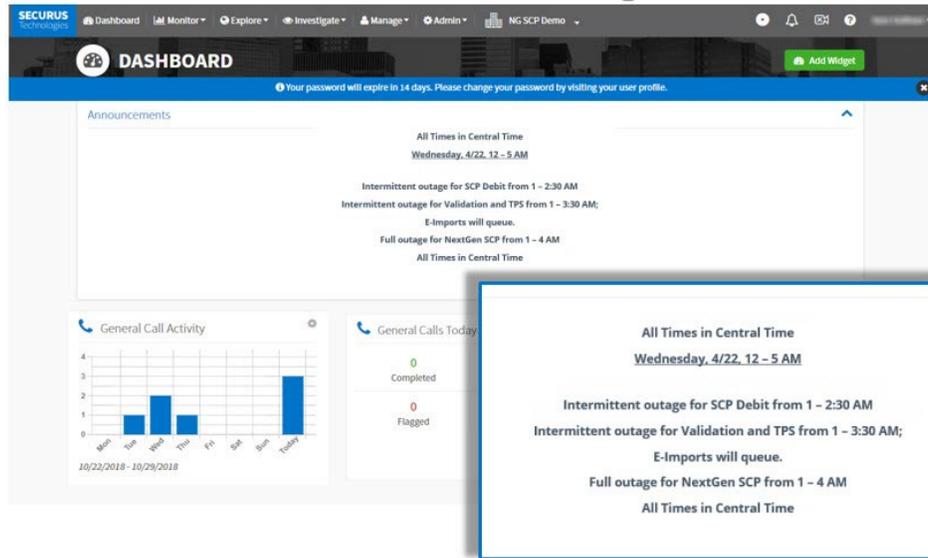
**Vendor should list client application deployment methods (please include how these applications will be updated).**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

After the initial installment, Securus delivers NextGen SCP software upgrades and systems updates to all customers three to four times per year with no downtime. Our updates keep pace with advances in technology and the evolving challenges in the corrections industry. More than just fixing glitches and small changes, these software updates deliver new features and capabilities.

**Minimize disruptions to communications and your work:** To deliver updates and perform maintenance events, Securus uses an after-hours process. Sedgwick County will be notified in advance of an upcoming system update; a notice of upcoming work is shown at login, and an announcement widget appears on the NextGen SCP dashboard with a link to summaries of upgrades and new features.

## Announcement Widget



### Wireless Updates and Integrated Antivirus protection

Updates to EVOTAB Tablets are done wirelessly. These updates include virus protection, application updates/upgrades, and patches, with no need to sync to external hardware. The EVOTAB firmware includes the antivirus protection for the tablets, so there is no need for a separate anti-virus program to be installed. With any new firmware release, it includes updated anti-virus protection.

**Vendor should list any included backup and recovery capabilities, objectives and estimated timelines. Please include any known issues with backup and recovery systems on the market.**

In the event of a disaster at a Securus data center, it will take the NextGen SCP platform 4 hours to recover from an alternate data center after a disaster has been declared. In the meantime, operations will shift to an operational data center.

### Comprehensive Disaster Recovery for Seamless Operations

Our Disaster Recovery Plan is designed for rapid response with unmatched service and support in any circumstance. Our goal is to prevent or minimize down-time and remove your administrative burdens. **Securus takes care of communications and technology while you take care of your population and facilities.**

- Robust network architecture designed to mitigate issues before they occur

- Field service team readily positioned close to your facilities and on-call 24/7
- A plan for escalating issues, adding resources, and recovering quickly

If a natural disaster or other significant adverse event occurs, Sedgwick County has the full support of the Securus Network Operations Center, the Securus Technical Support Team including engineering resources, and the Securus Field Service Team supported by a centralized field dispatch team. Our Field Service Technicians are fully trained in our disaster recovery plan and processes, and they are strategically positioned to support your ongoing maintenance and fast response in emergencies.

Response operations begin as soon as personnel safety is assured, and all emergency recovery operations are prioritized by critical facilities and equipment locations. For situations that are expansive in nature, we prioritize maximum-security sites and facilities with high offender phone usage.

## Three-Tiered Approach to Disaster Response and Recovery

### [1. Facility-Specific Emergency Response Checklists](#)

For every facility, we develop an emergency response checklist to protect equipment and personnel in the event of an emergency. These procedures may be as simple as using sandbags to stabilize equipment and placing tape on windows exposed to high winds. Your checklists will focus on mitigation and recovery with contingencies for extreme conditions such as earthquakes, flash floods, power outages, etc. Each checklist will be coordinated with Sedgwick County for consistency with your policy and procedures.

### [2. Systemwide Disaster Response Plan](#)

Securus works with you to declare emergencies for situations that are catastrophic and may impact a localized area or wide-spread region. Recovery plans are triaged based on the extent of impact and recovery operations may last a few hours, days, or weeks. Securus prioritizes recovery of premise-based equipment by facility type and equipment location. The Securus Local Recovery Team will continue recovery operations until operations are restored. Retrospective reports are completed for all declared emergencies to advance our emergency recovery planning efforts for the future.

### [3. A Foundation of Network and Equipment Preventative Measures](#)

Sedgwick County **avoids many communications-related disasters because we are prepared:** Securus provides a network and infrastructure tested to withstand adverse conditions, minimize outages, and protect your data. We research what works and then we

implement continuous improvements. Securus adds layers of redundancy at the local and national level to our core network and operations centers. We stock your facility and our Field Service Team with spare parts. We back up your data at three geographically diverse Securus data centers and layer redundancy throughout each component of our network. Information is routed through geographically diverse and route-diverse network paths, all while we monitor operations and communications 24x7x365.

Additional details on the Securus Disaster Recovery Plan and our preventative measures are outlined on the following pages. It's difficult to contemplate every contingency, but with 30+ years of experience providing communications and technology services to the corrections industry, **Securus has the experience to take care of Sedgwick County even when the unexpected occurs.**

### Sedgwick County Emergency Condition Declaration

**If you encounter a catastrophic adverse event or disaster at your facility, immediately call the Securus Emergency Numbers** that you are provided. Your call will be answered 24x7x365. Then with your Securus Account Manager you will request that Securus General Manager declare an emergency condition. Operations management then establishes an immediate conference bridge with the appropriate participants to gather information substantiating that an emergency status is warranted and determines the Disaster Level.

Securus classifies disasters on a Disaster Level Scale of 1-3:

- Level 1 Disasters are catastrophic events that are extremely wide-spread and affect many facilities and many customers.
- Level 2 Disasters are high-impact and affects a more wide-spread area than Level 3.
- Level 3 Disasters are moderate impact disasters typically affecting a localized area or specific facility with consideration that elevation of level may be needed.

**A single event trouble ticket is used to track all recovery efforts.** The Securus Technical Support Team will open a new trouble ticket in our ticket tracking system, indicating the declared condition level and the date and time of the declaration. All open tickets pertaining to the ongoing emergency recovery effort will be linked so that all recovery efforts are tracked as a single incident to facilitate complete resolution. This is critical for efficient and complete resolution in situations of extended recovery.

**If needed, Securus will deploy and pull resources from our nationwide network and engage our vendors to supply additional resources, equipment, or manpower.**

## EMERGENCY RESPONSE DISASTER LEVELS

### Disaster Level 1

Securus provides a full-headquarters response and may deploy a Headquarters Response Team to the region to coordinate and assist local recovery efforts. Securus Local Recovery Team activated, and your Account Manager will work with you to initiate a Command Center, including Securus Leadership. Necessary skill levels and geographic proximity are matched to your site's needs; additional personnel are dispatched as needed.

### Disaster Level 2

Securus Headquarters Response Team assists Securus Local Recovery Team as needed; onsite technician requirements assessed, and additional personnel dispatched as and when needed.

### Disaster Level 3

Securus Local Recovery Team coordinates all recovery operations. Headquarters assistance beyond standard Network Operations and Technical Support Teams likely not required.

## Risk Mitigation and Proactive Monitoring

**The Securus Network Operations Center (NOC) continuously monitors all data centers, infrastructure components, platform systems, and network/communication systems** using a suite of network performance monitors. The performance monitors are highly configurable to provide real-time monitoring, event notification, alert history, and statistical information. An alarm condition creates immediate visual alerts and email notifications.



The Securus NOC also monitors real-time video surveillance and environmental alerts for the Securus data centers. In the event there is an issue at the Securus Network Operations Center, **Securus maintains a fully redundant backup Network Operations Center at a separate physical location.**

**The Securus Technical Support Team monitors all facility-based equipment and connectivity 24x7x365** including firewalls, integrated access devices (IADs), visitation phone monitoring (VPM) units, routers, switches, on-site systems, wireless access points, user interfacing kiosks and terminals, and uninterrupted power supply (UPS) systems.

**The systems are polled every two minutes and their vital operating statistics sent every 10 minutes.** In addition to real-time monitoring and alerting, Securus Technical Support also leverages network performance monitor tools to gather and evaluate historical data for network alerts, bandwidth usage, packet loss, and hardware performance. This ongoing, proactive, in-depth analysis of your systems' performance enables our Technical Support Team to prevent and mitigate facility issues.

**Data storage redundancy is a key component of Securus' Risk Mitigation and Disaster Recovery Plan.** Securus maintains three data centers in geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.995% availability.

Securus' data centers meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier III, with some Tier IV (highest level) attributes, for data centers including:

- ability to withstand a 96-hour power event
- multi-layer physical security
- multiple power delivery paths

Each data center has redundant uninterrupted power systems, N+1 generator redundancy, and N+1 cooling redundancy. All systems and network equipment have redundant power paths. Multiple telecommunications carriers also serve each data center for load balancing and path diversity.

**Securus' data centers are staffed 24x7x365 for immediate physical assistance inside the data center.**

**Data is no longer susceptible to loss due to an individual drive failure or issues at your location:** The Securus communication platform uses technology that is much more advanced than traditional local onsite storage. Securus uses a mix of Storage Area Network (SAN)—a high-speed sub-network of shared storage devices—and Network-Attached Storage (NAS). This architecture avails all storage devices to all servers on Local Area Networks (LANs) or Wide Area Networks (WANs). Data is stored in Redundant Arrays of Independent Disk (RAID) formats, spreading the data across multiple drives, which provides additional protection. Accordingly, this architecture provides facilities with the ultimate protection against single drive or server failures, as well as increased security. **Securus maintains hardware replacement inventory on your site, in our Field Service Team vehicles, and at centralized locations.** In addition, we have distribution agreements with our vendors so that in the event of disaster recovery efforts, we can get replacement equipment to your facilities quickly.

## Localized Event Affecting Only Securus Facilities

In the event of a disaster impacting Securus, the local Securus Network and systems, or NextGen SCP, Securus immediately assembles a team of engineers to investigate and restore services. Securus maintains a schedule of on-call personnel for immediate response to service-impacting events and a list of third-party vendors to engage if needed. Our priority is fast resolution and minimal downtime. If a state of emergency is declared, the Securus Business Continuity Plan will be activated.

Upon confirmation of a service-impacting event, the Network Operations Center will issue an internal service interruption report (SIR). The SIR will include the nature of the outage, impact to facilities, and estimated time of restoration, if known. Each incident is assigned an urgency level based on the level of customer impact.

The Securus Executive Team and the Securus Account Management Team receive SIRs and communicate with you directly. In addition, the Securus Technical Support Team may communicate a service-impacting event via a splash screen on the NextGen SCP user interface introductory page. Securus updates you regularly throughout resolution. Securus investigates every service-impacting event, completes a root-cause analysis, and provides the analysis to you upon request.

## Data Protection through Redundant Storage

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

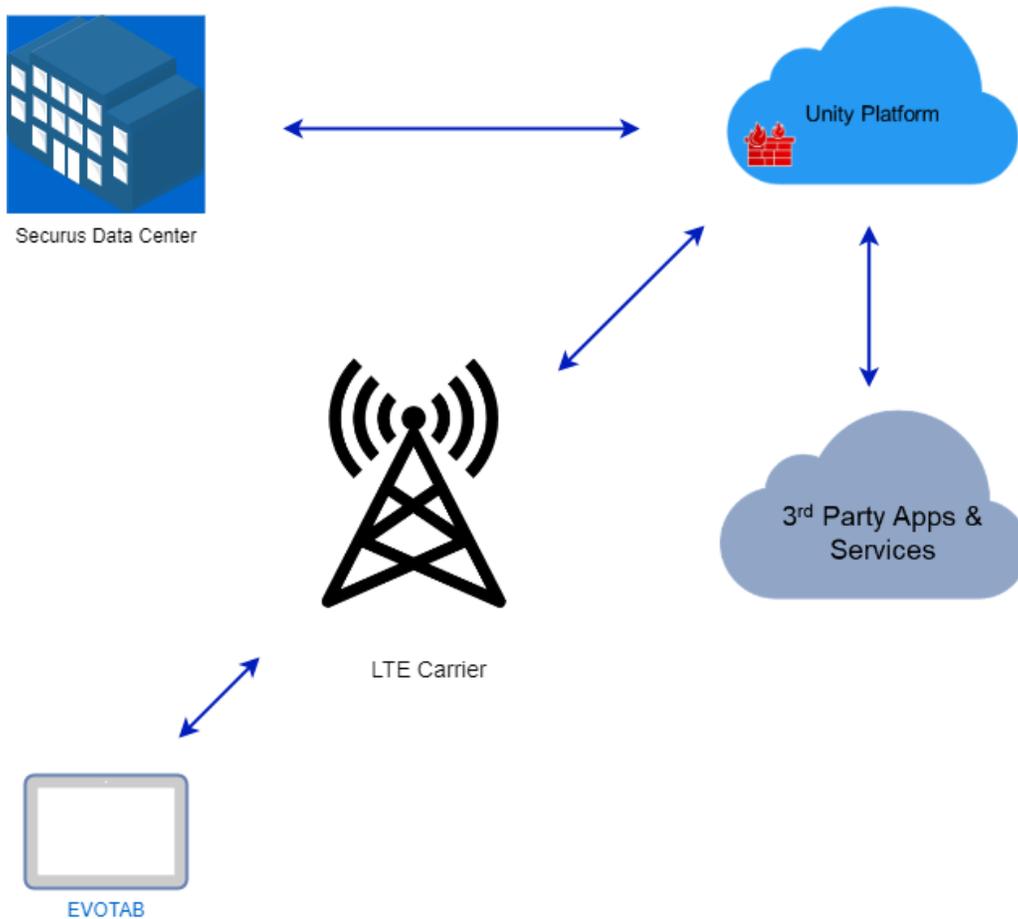
**Vendor should provide secure connections to data and be compliant with any regulatory requirements such as HIPAA, CJIS, and PCI requirements.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Vendor should include interface diagram and security specifics.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

EVOTAB is the corrections industry's first Google-certified tablet with cellular connection capability. The EVOTAB utilizes a secure VPN connection over the carrier's LTE network to connect to the Unity Platform and through it to the various Unity service offerings. The EVOTAB is managed by a Google certified Enterprise Mobility Management (EMM) tool that provides control over the tablet.



### EVOTAB Security

Both the EVOTAB hardware and software have industry-best security practices. Internet access is restricted, ensuring users can only visit authorized websites and cannot surf the internet or communicate through unauthorized channels with anyone outside of the facility. All of the infrastructure including the EVOTAB itself are monitored 24 x 7 to detect attempts to circumvent security controls. Customers are notified of any unusual activity within standard SLA times. Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.

## Tablet Hardware and Firmware

Securus EVOTAB is a corrections-grade hardened tablet that runs an android enterprise certified firmware created by our hardware partner. The features available in the firmware are controlled by the EMM also created by our hardware partner. The following security measures have been taken to harden the firmware on these tablets:

- The EMM controls what applications are installed and available to the user.
- Configuration settings have been restricted to only necessary settings.
- Authorized applications are pushed to the tablets through the EMM, thus preventing Incarcerated Individuals from installing or un-installing apps.
- Tablet network access is controlled by industry leading firewalls.
- Tablets are also prevented from accessing third-party app stores.

## LTE Access

The EVOTAB is pre-configured at the warehouse to connect to an authorized LTE carrier and is prevented from connecting to any other network through the security controls enforced via the EMM.

## Data Centers

Securus maintains a presence in multiple data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches, and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations

require anti-virus and anti-spyware protection software and the latest operating system patches.

**Securus provides multiple layers of security to ensure proper tablet usage and to prevent security breaches or tablet misuse.**

## Security Layer 1

### Tablet Firmware

Securus EVOTAB Tablets run a custom-developed proprietary firmware to harden their security and prevent any access to unauthorized content by the Inmates. The customized firmware does not have any of the common apps that are found on consumer-grade tablets.

The following security measures have been taken to harden the firmware on these tablets:

- Browser, contacts, calendar, native phone, and messaging clients have been removed.
- The option to change configuration settings has been removed.
- Near-field Communication (NFC) and Bluetooth have been disabled, except for Wi-Fi (where applicable/approved).
- Authorized applications are pushed to the tablets through Securus' app state management process, thus preventing Inmates from installing or un-installing apps.
- Tablets are prevented from accessing the public internet directly.
- Tablets are prevented from accessing third-party app stores.

### Wi-Fi Access

The firmware only allows the tablets to connect to a Securus-provided network using a unique SSID (Service Set Identifier) for Wi-Fi. Security mechanisms prevent the tablet from connecting to any other Wi-Fi network other than the one provided by Securus for exclusive use by the tablets.

Securus uses wireless access points (WAPs) that are customized only to broadcast the SSID to supported EVOTAB Tablets.

## Security Layer 2

### Securus Local Platform

All the WAPs are connected to a Securus Local Platform (SLP) running Securus' custom-developed proprietary software. These SLPs have components that inspect all the network

packets and provide firewall, transparent proxy, DHCP, DNS, and routing services for the tablets.

The SLP is essential to all tablet functions and is configured to govern what the tablets can access. The tablet cannot receive any content from a network that the SLP has not been configured to provide. The SLP inspects all tablets' traffic and ensures that access is granted only to authorized content.

Although a tablet can connect to the Wi-Fi network, it cannot obtain an IP (internet protocol) address unless it is recognized as an authorized device by the SLP. If a tablet is not known by the SLP, it will *not* be granted access to the wireless network and will be rendered useless for applications that require network connectivity.

The SLP at the facility premise is connected to Securus' data center over an Internet Protocol Security Virtual Private Network (IPsec VPN) tunnel. The IPsec VPN service provides secure IP communications by authenticating and encrypting each IP packet of a communication session.

## Security Layer 3

### Data Centers

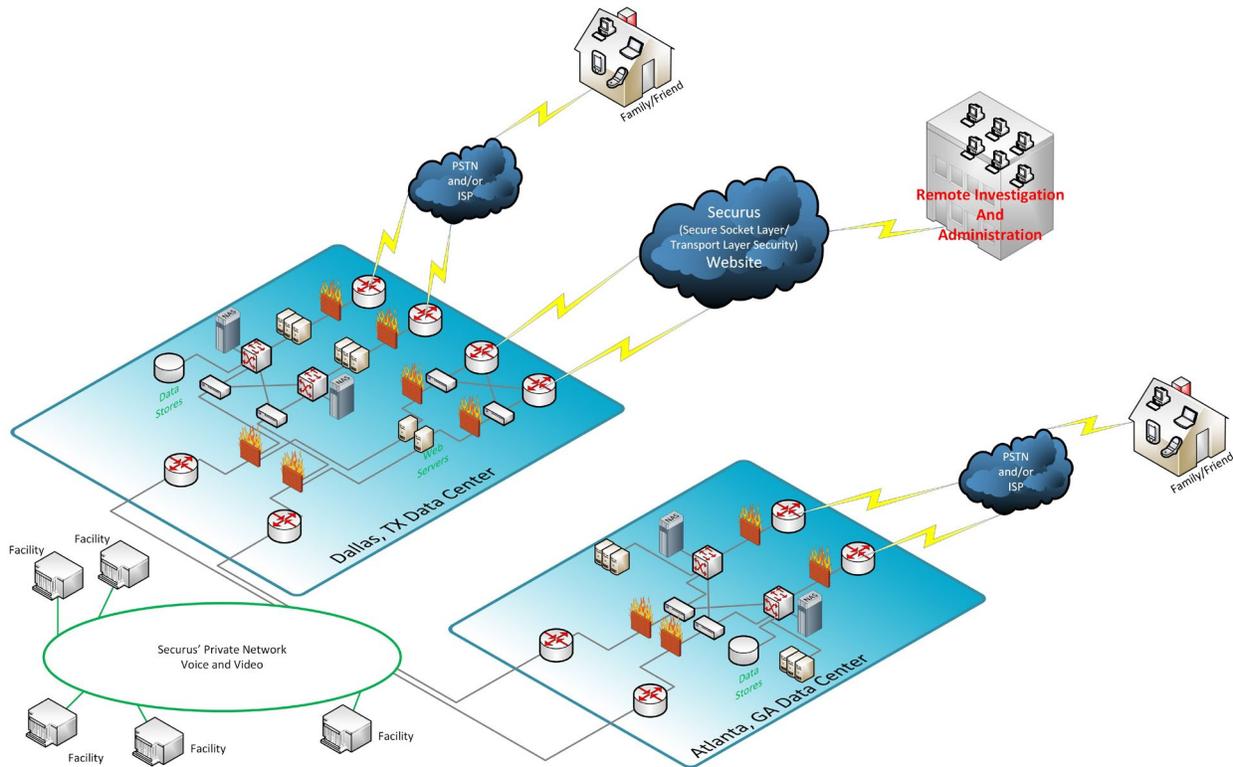
Securus maintains a presence in three data centers in two geographically diverse locations. Our data centers are designed to withstand worst-case events and maintain 99.99% availability. The data centers, managed and staffed by a carrier-class data center host, meet or exceed the Telecommunications Industry Association's (TIA) standard number 942 for Tier 4 (highest availability) data centers, including:

- Multiple power delivery paths
- Ability to withstand a 96-hour power event
- Two-hour fire protection
- Multi-layer physical security.

Multiple checks ensure data center physical security, including guarded, photo-verified check-in, dual-door authentication (card and biometric), and a mantrap (interlocking door controller) at the data center suite entrance.

Securus applies a high level of security to protect against cyber-attacks, and to secure its data. Applications transmitting data across public networks support SSL/TLS, Certificates, and 256-bit AES encryption. Routers, switches, and firewalls are used throughout the network to protect Securus and our customers. All servers, laptops, and workstations require anti-virus and anti-spyware protection software and the latest operating system patches.

Below is another diagram showing the secure transfer of data to and from Sedgwick County Detention Facility.



If not answered in previous question please list authentication and security methods for access to the system and system data.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Access to the system and system data requires a username and a password.

The software needs to be able to be supported on current technology standards and future / modern OS releases. Does this system stay up to date with modern software updates -- such as Windows OS or SQL versioning to the latest versions?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

Securus NextGen SCP is always up to date, offering Sedgwick County the latest the current technology. System upgrades are not provided by a Windows OS or SQL Version. NextGen SCP operates by accessing the internet through a web browser. All updates are handled over the internet.

Vendor should list Server and Client resource requirements (CPU, Memory, and Disk Space)

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

The only resource necessary to access NextGen SCP is an internet connection.

Vendor should indicate server and application update practices (Include the answers to how to patch the application on the client and server).

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus employs automated patch management systems for its servers and workstations. Systems are patched in keeping with industry standard patch cycles, and we have a patch management process for remediating unpatched systems within specific timelines. Securus exercises very aggressive patch management, which is an essential ingredient to a successful information security program. We are constantly patching servers and operating systems to assure we have the latest security updates, and as issues are discovered by regular vulnerability assessments.

Vendor should list network connection requirements.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

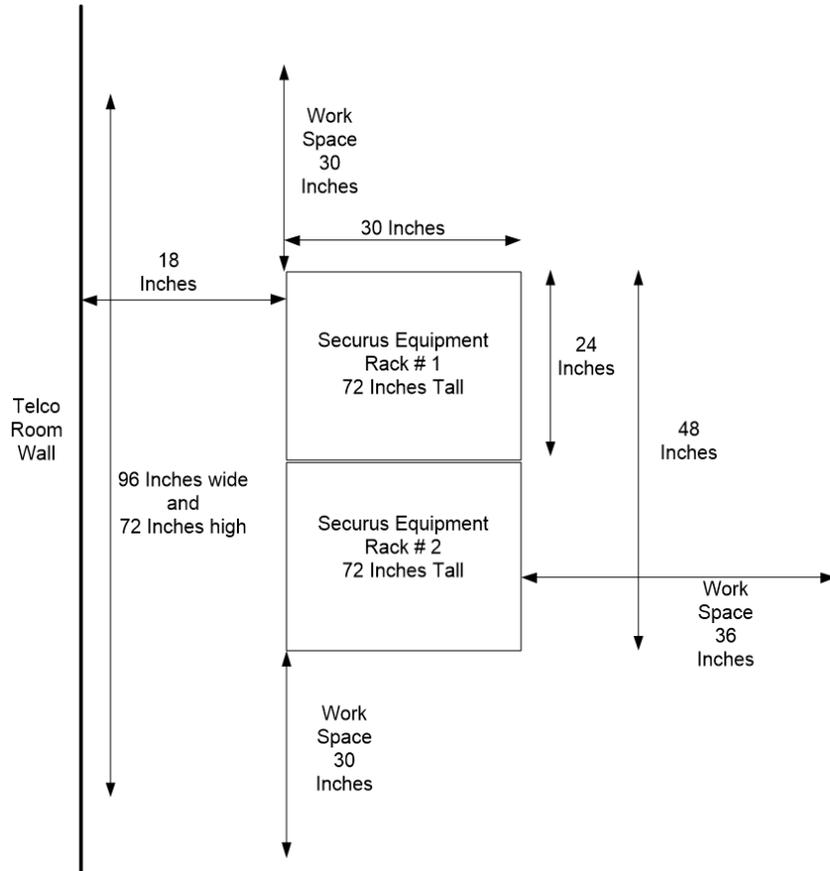
Securus provides all required network connectivity and does not require Sedgwick County to provide any network infrastructure.

If on premise, vendor should list system external interface requirements (Please include an interface diagram) – Is there any remote connection into the On-Premise system needed for support by the vendor?

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

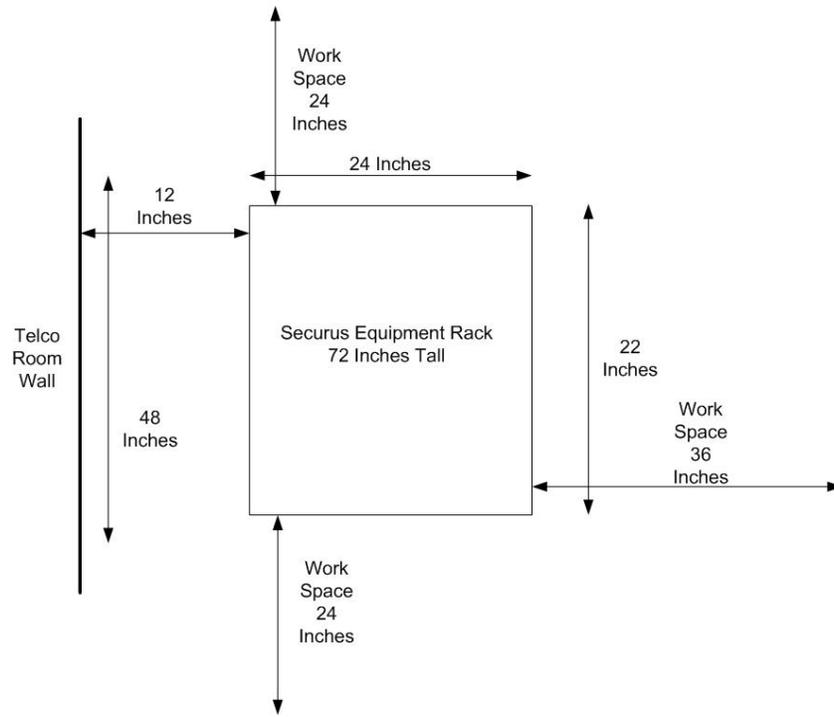
The following sample floor diagram illustrates the space requirements for our NextGen SCP system.

# Sample Floor and Wall Space Requirements



## Sample Floor and Wall Space Requirements

### Floor and Wall Space Requirements



If not addressed in previous response, vendor should list authentication and security methods for access to the system and system data.

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

Access to the system and system data requires a username and a password. Securus has recently enabled Multi-Factor Authorization (MFA) to access our systems.

Vendor should indicate backup methods recommended - any incompatibilities with backup systems on the market. Software should be compatible with modern antivirus clients (list any needed exceptions or known problems).

#### **SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

Securus provides all backup for Sedgwick County, so you don't have to handle this.

**Redundant protection against failures and disasters:** Each communication detail record (CDR), call recording, and video session recording is stored using a mix of file, block, and object-based Storage Area Network (SAN) and Network Attached Storage (NAS) technologies at our Data Centers in Dallas and Atlanta. Redundancy of storage locations

and storage using SAN/NAS technologies protects your data if there is a failure of an individual disk drive or a catastrophic event at one of our carrier-class Data Centers. In addition, all CDRs are backed up to tape at a third site, an additional layer of geographic redundancy. Traditional local facility-based storage systems are susceptible to local catastrophic events and disasters and require a manual backup program. Securus Data Centers and the Securus storage infrastructure is monitored and managed 24x7x365 by our Network Operations Center. **Securus Data Centers provide a higher level of security for your data.**

For on premise solutions, Vendor should provide full instructions for configuring database connection strings.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus does not provide on-premise solutions. Therefore, this question is not applicable.

For on premise solutions, Vendor should provide a list of supported and compatible database system versions.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus does not provide on-premise solutions. Therefore, this question is not applicable.

## PROJECT STATUS REPORTING

Weekly written status reports shall be submitted to the Department Project Manager. These status reports should outline:

- a. Overall summarization of the project progress;

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- b. Deliverables achieved;

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- c. Deliverables remaining, progress, and expected delivery on each; and

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

- d. Issues and concerns affecting specific deliverables and the project schedule or any other aspect of the project.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. CHANGED ANSWER**

## ACCEPTANCE TESTING

- a. The vendor will work with the department to create an acceptance testing plan. Both parties shall agree to the plan in writing and the plan must be completed prior to county acceptance of the solution.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## DOCUMENTATION

- a. The vendor shall provide system documentation (written or electronic) to the department. This will include a detailed description of each solution.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## USER TRAINING

- a. Initial training will be provided, on site, by the vendor for all communication services.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADD TRAINING MODELS**

- b. Vendor shall provide a detailed summary of the training plan.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADD TRAINING TEAM AND STATEMENT**

- i. Vendor must describe its training philosophy and provide detailed training plans of all topics covered.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADD TRAINING APPROACH FROM TEAM AND AGAIN ALL TOPICS COVERED**

- c. In addition to initial training required at the time of system installation, if deemed necessary by Sedgwick County the vendor must offer and provide additional training to existing or new Sedgwick County employees.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADDITIONAL TRAINING AND ONLINE OPTIONS**

- i. Please describe follow-up training options, such as, on-site or webinar training if available.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADD ONLINE OPTION**

- d. All training will be provided at no additional cost to the county.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY. - ADD ONGOING STATEMENT**

## VI. SEDGWICK COUNTY RESPONSIBILITIES

- Provide information, as legally allowed, in possession of the county, which relates to the county's requirements or which is relevant to this project.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus understands that Sedgwick County will provide us with the information, as legally allowed, in possession of the county, which relates to the county's requirements or which is relevant to this project.

- Designate a person to act as the county Contract Manager with respect to the work to be performed under this contract.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus understands that Sedgwick County will designate a person to act as the county Contract Manager with respect to the work to be performed under this contract.

Michael Love, is the Primary Contact for Sedgwick and would act as the Contract Manager in respect to the work performed under this contract. His contact information is [michael.love@securustechnologies.com](mailto:michael.love@securustechnologies.com) or (460) 540-0006.

- Conduct final inspection

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus understands that Sedgwick County will conduct a final inspection.

## VII. PROPOSAL TERMS

### A. Questions and Contact Information

Any questions regarding this document must be submitted via email to Lee Barrier at [Lee.Barrier@sedgwick.gov](mailto:Lee.Barrier@sedgwick.gov) by 5:00 pm CDT October 4, 2024. Any questions of a substantive nature will be answered in written form as an addendum and posted on the purchasing website at <https://www.sedgwickcounty.org/finance/purchasing/requests-for-bid-and-proposal/> under the Documents column associated with this RFP number by 5:00 pm CDT, October 18, 2024. Firms are responsible for checking the website and acknowledging any addenda on their proposal response form.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

### B. Minimum Firm Qualifications

This section lists the criteria to be considered in evaluating the ability of firms interested in providing the service(s) and/or product(s) specified in this Request for Proposal. Firms must meet or exceed these qualifications to be considered for award. Any exceptions to the requirements listed should be clearly detailed in proposer's response. Proposers shall:

1. Have a minimum of 10 years' experience in providing services similar to those specified in this RFP.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has 10 years of experience providing services similar to those specified in this RFP. Please see our response to Requirement 1 in Section VII for more information.

2. **Have experience in managing projects of comparable size and complexity to that being proposed.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has experience managing project of comparable size and complexity to that being proposed in this RFP. Please see our response to Requirement 1 in Section VII for more information.

3. **Have knowledge of and comply with all currently applicable, and as they become enacted during the contract term, federal, state and local laws, statutes, ordinances, rules and regulations. All laws of the State of Kansas, whether substantive or procedural, shall apply to the contract, and all statutory, charter, and ordinance provisions that are applicable to public contracts in the county shall be followed with respect to the contract.**

**4. SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus is committed to working closely with Sedgwick County to establish contract terms that are mutually agreed upon, ensuring compliance with all applicable federal, state, and local laws, statutes, ordinances, rules, and regulations. We recognize the importance of adhering to the laws of the State of Kansas and will diligently follow all relevant statutory, charter, and ordinance provisions applicable to public contracts throughout the duration of our partnership.

5. **Municipal and county government experience is desired, however, the county will make the final determination based on responses received and the evaluation process.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus acknowledges the importance of municipal and county government experience and is prepared to provide relevant insights and expertise. We understand that Sedgwick County will make the final determination based on the responses received and the evaluation process, and we are committed to demonstrating our qualifications to meet your needs. Please reference Requirement 1 in Section VII for more information.

6. **Have the capacity to acquire all bonds, escrows or insurances as outlined in the terms of this RFP.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has the capacity to acquire all necessary bonds, escrows, and insurances as outlined in the terms of this RFP. We are fully prepared to meet the requirements to ensure a secure and compliant partnership.

**7. Provide project management (as required) and quality control procedures.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has provided project management and quality control procedures in our implementation plan located on our response to requirement 11 in the System Architecture and Design section.

**8. Have appropriate material, equipment and labor to perform specified services.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has the appropriate material, equipment and labor to perform specified services.

**9. Park only in designated areas and display parking permit (if provided).**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus employees will only park in designated areas and display parking permit if needed.

**10. Wear company uniform and ID badge for identification purposes.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus employees will wear company uniform and ID Badge for identification purposes.

**C. [Evaluation Criteria](#)**

The selection process will be based on the responses to this RFP. County staff will judge each response as determined by the scoring criteria below. Purchasing staff are not a part of the evaluation committee.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Component	Points
A. Demonstrated ability to meet the technical requirements, based upon the RFP responses and information provided by similar facilities in which the vendor has their system installed.	30
B. Rates charged to party who accepts charges.	20
C. Vendor experience, technology offering, account support team, maintenance and current customer references.	30
D. Proposed project plan, scheduling and implementation with minimal interruption of service.	20
Total Points	100

Assume the following cost proposals (examples only)

- A. \$50,000.00
- B. \$38,000.00
- C. \$49,000.00

Company B with a total price of \$38,000.00 is the low offer. Take the low offer and divide each of the other offers into the low offer to calculate a percentage. This percentage is then multiplied by the number of points available for the cost. In this case, 10 points are allocated to cost.

- A.  $\cdot \$38,000.00 \text{ divided by } \$50,000.00 = .76$        $.76 * 10 = 7.6$  points
- B.  $\cdot \$38,000.00 \text{ divided by } \$38,000.00 = 1.00$        $1.00 * 10 = 10$  points
- C.  $\cdot \$38,000.00 \text{ divided by } \$49,000.00 = .77$        $.77 * 10 = 7.7$  points

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please reference Attachment G for Securus' MWRA compliant Cost Proposal.

Any final negotiations for services, terms and conditions will be based, in part, on the firm's method of providing the service and the fee schedule achieved through discussions and agreement with the county's review committee. The county is under no obligation to accept the lowest priced proposal and reserves the right to further negotiate services and costs that are proposed. The county also reserves the sole right to recommend for award the proposal and plan that it deems to be in its best interest.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

The county reserves the right to reject all proposals. All proposals, including supporting documentation shall become the property of Sedgwick County. All costs incurred in the

preparation of this proposal shall be the responsibility of the firm making the proposals. Sedgwick County reserves the right to select, and subsequently recommend for award, the proposed service which best meets its required needs, quality levels and budget constraints.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**D. Request for Proposal Timeline**

The following dates are provided for information purposes and are subject to change without notice. Contact the Purchasing Department at (316) 660-7255 to confirm any and all dates.

Distribution of Request for Proposal to interested parties	September 6, 2024
Mandatory Pre-Proposal Meeting	September 18, 2024
Questions and clarifications submitted via email by 5:00 pm CDT	October 4, 2024
Addendum #3 Issued by 5:00 pm CST	November 19, 2024
Revised /New Proposals due before 1:45 pm CST	December 3, 2024
Evaluation Period	December 4, 2024 - December 23, 2024
Board of Bids and Contracts Recommendation	January 9, 2025
Board of County Commission Award	January 15, 2025

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**E. Request for Proposal Timeline**

A contractual period will begin following Board of County Commissioners (BoCC) approval of the successful firm(s) and continue for a period of three (3) years with three (3) one (1) year options to renew.

County may cancel its obligations herein upon thirty-day (30) prior written notice to the other party. It is understood that funding may cease or be reduced at any time, and in the event that adequate funds are not available to meet the obligations hereunder, either party reserves the right to terminate this agreement upon thirty (30) days prior written notice to the other. Payment will be remitted following receipt of monthly detailed invoice.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Payment and Invoice Provisions

<https://www.sedgwickcounty.org/media/55477/payment-and-invoice-proviions.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**F. Insurance Requirements**

Liability insurance coverage indicated below must be considered as primary and not as excess insurance. If required, contractor’s professional liability/errors and omissions insurance shall (i) have a policy retroactive date prior to the date any professional services are provided for this project, and (ii) be maintained for a minimum of three (3) years past completion of the project. Contractor shall furnish a certificate evidencing such coverage, with county listed as an additional insured including both ongoing and completed operations, except for professional liability, workers’ compensation and employer’s liability. Certificate shall be provided prior to award of contract. Certificate shall remain in force during the duration of the project/services and will not be canceled, reduced, modified, limited, or restricted until thirty (30) days after county receives written notice of such change. All insurance must be with an insurance company with a minimum BEST rating of A-VIII and licensed to do business in the State of Kansas (must be acknowledged on the bid/proposal response form).

NOTE: If any insurance is subject to a deductible or self-insured retention, written disclosure must be included in your proposal response and also be noted on the certificate of insurance.

It is the responsibility of contractor to require that any and all approved subcontractors meet the minimum insurance requirements.

<b>Workers’ Compensation:</b>	
Applicable coverage per State Statutes	
Employer’s Liability Insurance:	\$500,000.00
<b>Commercial General Liability Insurance (on form CG 00 01 04 13 or its equivalent):</b>	
Each Occurrence	\$1,000,000.00
General Aggregate, per project	\$2,000,000.00
Personal Injury	\$1,000,000.00
Products and Completed Operations Aggregate	\$2,000,000.00
<b>Automobile Liability:</b>	
Combined single limit	\$500,000.00
<b>Umbrella Liability:</b>	
Following form for both the general liability and automobile	
<input checked="" type="checkbox"/> Required / <input type="checkbox"/> Not Required	
Each Claim	\$1,000,000.00
Aggregate	\$1,000,000.00
<b>Professional Liability/ Errors &amp; Omissions Insurance:</b>	
<input checked="" type="checkbox"/> Required/ <input type="checkbox"/> Not Required	
Each Claim	\$1,000,000.00
Aggregate	\$1,000,000.00



<b>Builder’s Risk Insurance:</b>	<b>In the amount of the initial Contract Sum, plus the value of subsequent modifications and cost of materials supplied and installed by others, comprising the total value for the entire Project on a replacement cost basis without optional deductibles. Entity, contractor, and all Subcontractors shall be included as named insured’s.</b>
----------------------------------	---

**SECURUS HAS READ, UNDERSTANDS, AND WILL PARTIALLY COMPLY.**

Securus Technologies does not require Builder’s Risk Insurance, as we will not be performing any construction services as part of this contract. Our focus is on providing technology solutions, and our activities do not involve the installation or modification of physical structures that would necessitate this type of insurance.

We are committed to maintaining compliance with all applicable insurance requirements relevant to our services. If you have any questions or need further clarification regarding our insurance policies, please feel free to reach out.

**G. Indemnification**

To the fullest extent of the law, the provider, its subcontractor, agents, servants, officers or employees shall indemnify and hold harmless Sedgwick County, including, but not limited to, its elected and appointed officials, officers, employees and agents, from any and all claims brought by any person or entity whatsoever, arising from any act, error, or omission of the provider during the provider’s performance of the agreement or any other agreements of the provider entered into by reason thereof. The provider shall indemnify and defend Sedgwick County, including, but not limited to, its elected and appointed officials, officers, employees and agents, with respect to any claim arising, or alleged to have arisen from negligence, and/or willful, wanton or reckless acts or omissions of the provider, its subcontractor, agents, servants, officers, or employees and any and all losses or liabilities resulting from any such claims, including, but not limited to, damage awards, costs and reasonable attorney’s fees. This indemnification shall not be affected by any other portions of the agreement relating to insurance requirements. The provider agrees that it will procure and keep in force at all times at its own expense insurance in accordance with these specifications.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**H. Confidential Matters and Data Ownership**

The successful proposer agrees all data, records and information, which the proposer, its agents and employees, which is the subject of this proposal, obtain access, remains at all times exclusively the property of Sedgwick County. The

successful proposer agrees all such data, records, plans and information constitutes at all times proprietary information of Sedgwick County. The successful proposer agrees that it will not disclose, provide, or make available any of such proprietary information in any form to any person or entity. In addition, the successful proposer agrees it will not use any names or addresses contained in such data, records, plans and information for the purpose of selling or offering for sale any property or service to any person or entity who resides at any address in such data. In addition, the successful proposer agrees it will not sell, give or otherwise make available to any person or entity any names or addresses contained in or derived from such data, records and information for the purpose of allowing such person to sell or offer for sale any property or service to any person or entity named in such data. Successful proposer agrees it will take all reasonable steps and the same protective precautions to protect Sedgwick County's proprietary information from disclosure to third parties as with successful proposer's own proprietary and confidential information. Proposer agrees that all data, regardless of form that is generated as a result of this Request for Proposal is the property of Sedgwick County.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

I. [Proposal Conditions](#)

<https://www.sedgwickcounty.org/media/31338/proposal-terms-conditions.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

General Contract Provisions

<https://www.sedgwickcounty.org/media/31337/general-contractual-provisions.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Mandatory Contract Provisions

<https://www.sedgwickcounty.org/media/31336/mandatory-contractual-provisions.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Independent Contractor

<https://www.sedgwickcounty.org/media/54780/independent-contractor-addendum.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL PARTIALLY COMPLY.**

8. "Warranties and Representations. Goods or equipment delivered and/or services rendered hereunder must be made according to the terms of this Agreement both as to time and quantities, with County reserving the right to cancel, reject or refuse any delivery made and/or service rendered prior to or subsequent to the times specified. In the event

no quality is specified on the face hereof, the goods or equipment delivered and/or services rendered hereunder must be of the best quality. If delivery of goods or equipment and/or rendering of services cannot be maintained, Contractor must notify County immediately. Upon Contractor's failure to maintain delivery or otherwise perform hereunder, County reserves the right to procure such goods or equipment and/or services elsewhere, in whole or in part, and assess Contractor with any additional costs incurred, unless Contractor's default arises from causes beyond its control and without fault or negligence. This remedy is in addition to any other remedy which County may have pursuant to this Agreement or otherwise and/or any warranty that may be implied or imposed by operation of law."

**SECURUS HAS READ AND UNDERSTANDS.**

**DUE TO THE SUBSTANTIAL UPFRONT INVESTMENT WE MAKE TO INSTALL AND MAINTAIN YOUR SYSTEM, SECURUS WOULD REQUEST A 30-DAY CURE PERIOD FROM RECEIPT OF THE LETTER TO CORRECT ANY ISSUES AND MUTUALLY AGREE WITH THE COUNTY PRIOR TO THE COUNTY PROCURING THIRD-PARTY EQUIPMENT.**

10.A. "Termination for Cause. In the event of any breach of the terms or conditions of this Agreement by Contractor, or in the event of any proceedings by or against Contractor in bankruptcy or insolvency or for appointment of receiver or trustee or any general assignment for the benefit of creditors, County may, in addition to any other remedy provided it by law or in equity or other right reserved to it elsewhere in this Agreement, without any liability to Contractor on account thereof, by written notice, terminate immediately all or any part of this Agreement, procure the goods, equipment and/or services provided for herein elsewhere, on such terms and under such conditions as are reasonable in the sole discretion of County, and Contractor shall be liable to pay to County any excess cost or other damages caused by Contractor as a result thereof."

**SECURUS HAS READ AND UNDERSTANDS.**

**DUE TO THE SUBSTANTIAL UPFRONT INVESTMENT THAT WE MAKE INSTALLING AND MAINTAINING YOUR INMATE COMMUNICATION SYSTEM, SECURUS RESPECTFULLY REQUESTS A 30-DAY CURE PERIOD, WITH AN ADDITIONAL 90-DAY PERIOD IF THE BREACH CANNOT BE REASONABLY CURED WITHIN 30 DAYS, SO LONG AS WE ARE DILIGENTLY WORKING THROUGH CURING THE BREACH THE WHOLE PERIOD.**

Sample Contract

<https://www.sedgwickcounty.org/media/39236/sample-contract.pdf>

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Federal Certifications Addendum Sedgwick County

<https://www.sedgwickcounty.org/media/59719/federal-certifications-addendum-updated-for-changes-to-ug-11-12-2020-no-signature-line.pdf>  
**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

**Suspension and Debarment**

<https://www.sedgwickcounty.org/finance/purchasing/suspension-and-debarment/>  
**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

## VIII. REQUIRED RESPONSE CONTENT

All proposal submissions shall include the following:

1. Firm profile: the name of the firm, address, telephone number(s), contact person, year the firm was established, and the names of the principals of the firm.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Sr. Account Manager, Michael Love, will be the primary contact for Sedgwick County. He may be reached directly at [michael.love@securustechnologies.com](mailto:michael.love@securustechnologies.com) or 972-277-0413.

### Securus

The Securus corporate headquarters is located at 5360 Legacy Drive, Suite 300, Plano, Texas 75024.

At Securus, our vision is to equip every public safety, law enforcement, and corrections agency throughout the world with our civil and criminal justice technology solutions. Securus' powerful, connected technology protects the world and drives continuous innovation with an exceptional focus on solutions that best serve our customers.

#### **SECURUS AT A GLANCE**

30+ years in business

1300+ employees

approximately 1,800 installed sites

297+ million completed calls for the past twelve months

99.9% network uptime

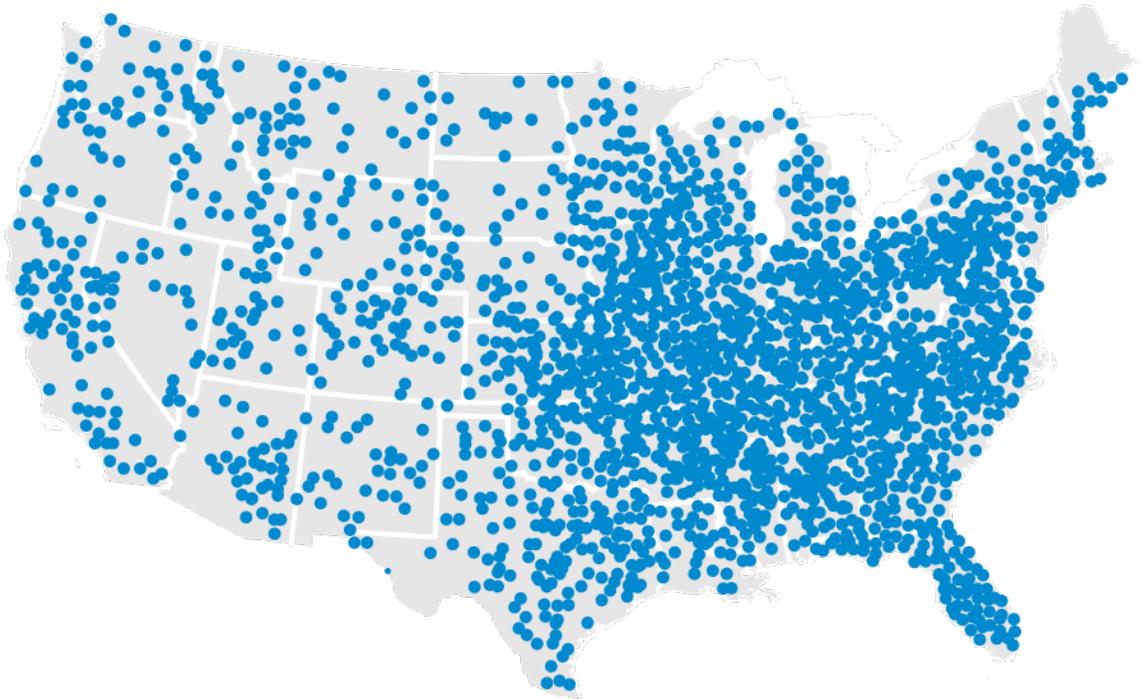
310 patents issued with 246 currently in force

89% customer retention rate

## Our Presence

For 30+ years, facilities, inmates, and the family and friends of inmates have relied on our communication solutions designed to fulfill their needs. We continue to leverage our technical expertise and expand our portfolio with complementary products and services that go beyond communications.

We have the resources to install and operate jail and prison facility telecommunications systems, from the smallest facilities to the largest DOCs, including Florida DOC; Louisiana DOC; Missouri DOC; Illinois DOC; Kentucky DOC; Pennsylvania DOC; Connecticut DOC; New York City DOC; Boston, Massachusetts; Denver, Colorado; Dallas, Texas; Seattle, Washington; and Portland, Oregon. We are uniquely equipped to handle any inmate population.



*Locations served by Securus Technologies*

## Our Values

Our culture focuses on people being innovative, exceptional, focused, and trustworthy. These characteristics actively contribute to the company's long-term success and explain the passion Securus has for technological advancements and outstanding service. Below are our core values:

### TRUSTWORTHY

*Securus strives to operate with transparency and embodies the highest levels of integrity, honesty, and truthfulness.*

### FOCUSED

*Securus focuses on delivering products and services that align with our overarching vision – ensuring our world is secure.*

### EXCEPTIONAL

*Securus is committed to delivering the best solutions comprised of the industry's best technology, products, and services.*

### INNOVATIVE

*Securus leads the industry in investments to support ongoing technological advancements – resulting in numerous patents. We combine information, product features, and services in a customized way to meet the unique needs of every customer.*

## What We Do

We can provide a full spectrum of civil and criminal justice technology solutions.



INVESTIGATIVE SOLUTIONS	CORRECTIONS SOLUTIONS	MONITORING SOLUTIONS
<p><b><i>Digital evidence is everywhere.</i></b></p> <p>Systems that merge big data, voice biometrics, and pattern identification, providing early detection and alerts for investigators, attorneys, courts and criminal justice systems.</p>	<p><b><i>Technology eases operational burdens.</i></b></p> <p>Systems that modernize the incarceration experience through jail management, communications, and Inmate self-service to help Inmates communicate with their family, friends, and corrections agencies run smoothly and reduce recidivism.</p>	<p><b><i>Community supervision reduces cost.</i></b></p> <p>Systems that combine intuitive software, dependable hardware, and comprehensive support services to more effectively monitor and track offenders, increase compliance, reduce recidivism, and maintain public safety.</p>

## Why Securus

As you review our proposal, you will see recurring themes that separate Securus from our competitors:

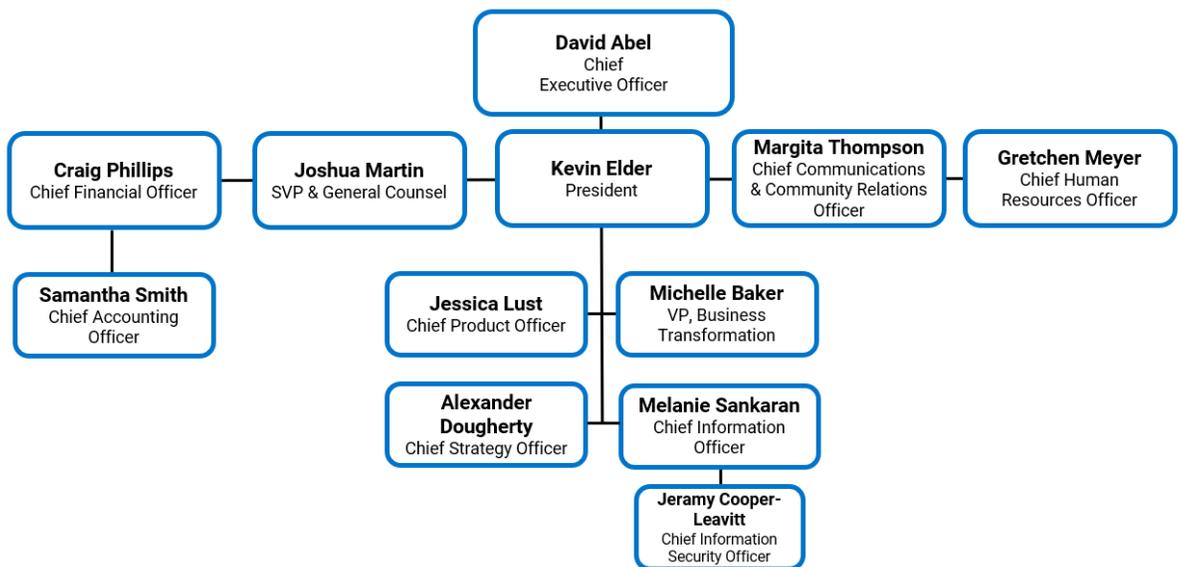
- **Experience:** We provide services to four of the top five mega county facilities in the United States. We serve multiple DOCs, including the state of Kansas. We also serve other very large facilities that house thousands of inmates, including New York City DOC; and Dallas County, Texas. Not to be forgotten, we also serve many small counties and cities, which have needs unique to smaller facilities. Our experience allows us to adapt to the size of our customers and their needs.
- **Technology:** We are a true technology company. We invest heavily in technology and lead the market in innovation. We do this because we believe technology has and will continue to revolutionize the corrections experience, creating safer facilities, improving reentry, reducing recidivism, and increasing operational efficiencies.
  - Our widely used, flexible and dynamic communication platform has the features and investigative tools you need to keep your community safe.

- We have a variety of corrections solutions that reduce workload, increase safety & security, and provide jail staff and inmates unprecedented communication access.
- Our commitment to technology means that we'll continue to innovate and provide you with cutting-edge solutions, now and throughout the term of our agreement.
- **Service:** Our 89% customer retention rate, shows we listen closely to, and continuously adapt to our customers' needs.
  - We offer a variety of programs to complete more calls than any other competitor in the industry. Your inmates' families and loved ones are also our customers and they play a critical role in the rehabilitation of inmates by staying in contact during incarceration. This is why we provide multiple ways to communicate and provide more funding options than any other provider. We routinely improve call volumes when we displace our competition, making sure inmates can stay in touch with their loved ones.

## Leadership Team

The Securus Executive Leadership Team reports to the President and Chief Executive Officer. The Leadership Team consists of diverse and experienced innovators dedicated to delivering reliable and cost-effective communication and technology solutions within the corrections industry.

Securus Organization Chart



## Executive Members

**David Abel, Chief Executive Officer**, has 30+ years of public and private sector technology experience including criminal justice, law enforcement, national security, and intelligence. Dave started a successful automation and artificial intelligence business, was a partner at PricewaterhouseCoopers, and was an executive in the U.S. and overseas with IBM where he was the General Manager, U.S. Public Sector, with revenue over \$2 billion and a team of more than 4,000.

- B.S., Commerce, University of Virginia

**Kevin Elder, President**, is a 20-year veteran of the technology and telecommunications industry, coming from IBM, where he most recently served as Managing Partner and General Manager of the Communications Market for IBM Services, North America, leading the Fortune 50's telecommunications, media and entertainment, and energy and utilities sectors. In this role, Kevin was a member of the North American and Global Operating Committees, a champion of workplace diversity, and an active mentor developing talent across IBM's North American footprint. Kevin leads Securus' day-to-day operations, partnering with our talent to reimagine and redefine our process and service delivery approach.

- B.B.A., University of Texas at Arlington
- Texas Tech University – Rawls College of Business

**Craig Phillips, Chief Financial Officer**, has accumulated more than three decades of experience with several organizations, including more than 15 years in "Big 4" public accounting firms serving large public and privately held high-growth companies in a broad spectrum of industries. Over the course of his career, Craig has assisted companies in the execution of public and private offerings of debt and equity securities, as well as numerous purchase and sale transactions. He has served as Chief Financial Officer for several public and privately held companies at the regional and national level in the manufacturing, service, distribution, entertainment, and restaurant industries, and recently served as the Chief Financial Officer of Purple Innovation.

- B.B.A. – Accounting, University of Georgia

**Jessica Lust, Chief Product Officer**, has 15+ years of experience leading projects and teams in the brand merchandizing and telecommunications industries. In

addition, she previously served as the Director of Client Services for JPay, Inc., a Securus subsidiary and the industry leader in corrections communications and payment technology.

- B.A., Marketing and Economics, Coastal Carolina University

**Alex Dougherty, Chief Strategy Officer**, is an experienced strategist and change leader. He began his career in financial analysis in the defense industry and then guided transformation in diverse industries while in leadership roles at a leading consulting company. Prior to joining the Securus Team, Alex was Vice President, Transformation, at Platinum Equity, the private equity owner of Securus.

- B.B.A., Finance, Texas Tech University
- M.B.A., Finance, Southern Methodist University

**Josh Martin, Senior Vice President and General Counsel**, is an attorney with 20+ years of experience advising companies on dispute resolution and strategic initiatives. Prior to joining Securus in 2016, Josh practiced as a commercial litigator with global law firms, and he excels at finding creative, practical, and business-oriented solutions to complex legal problems.

- J.D., University of California, Berkeley—School of Law
- B.A., Political Science, San Diego State University

**Melanie Sankaran, Chief Information Officer**, is an industry recognized cybersecurity leader with 20+ years of experience across multiple industries and technology layers. Previous roles include Vice President of Cyber Operations at Fidelity Investments and leadership at Experian where she directed Information Security for North America and Application Security globally. Melanie also held various information security roles at Wells Fargo Dealer Services, Foundstone, and Ernst & Young.

- B.B.A., Information Systems and Management, University of Cincinnati College of Business

**Jeremy Cooper-Leavitt, Chief Information Security Officer**, has 20+ years of international success in implementing strategic-level IT plans including network migration, security consulting, SOX compliance implementations, IT Governance, Payment Card Industry Compliance, and Privacy Law compliance (International and

US privacy laws). He has been instrumental in developing the Cyber program, bringing stability and acceleration to key initiatives and overall leadership of the team since joining Securus.

- M.I.S.M., Masters of Information Systems Management, Brigham Young University
- B.S., Information Systems, Brigham Young University
- A.S., Business Management, Rick's Junior College

**Samantha Smith, Chief Accounting Officer**, has 18+ years of experience with several organizations, including five years in "Big 4" public accounting and global consulting firms serving large public and privately held companies in a broad spectrum of industries. She is a licensed certified public accountant in the state of Texas. In addition, she previously served as the Global Controller, SVP, at an automotive technology company.

- B.S., Accounting – University of South Florida
- Master of Science, Accounting – University of Notre Dame

**Margita Thompson, Chief Communications and Community Engagement Officer**, has 25+ years of communications, public policy, and community engagement experience across federal, state, and local governments. In the private sector, she has worked in industries crossing energy, entertainment, real estate, and technology. Among previous positions, she served as Press Secretary for California Governor Arnold Schwarzenegger, political producer at CNN for Larry King Live, and as a public affairs leader at Fortune 500 companies, including Disney and Health Net. Most recently, Margita was Senior Vice President of US Corporate Communications at Unibail-Rodamco-Westfield.

- B.A., University of California, Berkeley
- M.P.P., Harvard University Additional Senior Leadership Members

**Michelle Baker, Vice President—Business Transformation**, is a Strategy Executive with over 25 years of experience specializing in aligning organizations to a Centralized Vision then driving strategic initiatives to achieve their goals. For the last 10 years she has specialized in Telecommunications supporting Comcast Cable and Cox Communications in driving transformation programs. Before Telecom, she worked in Strategy and Finance roles with The Coca-Cola Company, Fleetcor, AHL Services and The Federal Reserve Bank of Atlanta. Michelle is passionate about

untapping the potential in people and enjoys mentoring entrepreneurs and start-up companies. Michelle leads the strategic transformation efforts and business intelligence for Securus.

- Executive MBA - Emory University
- BS Finance & BA Economics – University of Florida

**Gretchen Meyer, Chief Human Resources Officer**, is a nationally recognized HR executive with an extensive background in development and implementation of total wellness programs, which drive positive outcomes on company success while improving the employee experience. Gretchen has more than 20 years’ experience working for large corporations including Novartis, Alcon Laboratories, and Lockheed Martin.

- B.A., College of Saint Mary's, Omaha, Nebraska

2. The firm’s relevant experience, notably experience working with government agencies.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please reference response above.

3. At minimum, three (3) professional references from facilities with a minimum of 500 beds, with email addresses, telephone numbers, and contact persons where work has been completed within the last three (3) years.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

• CLIENT REFERENCE 1	
Facility Name	Elkhart County, IN
Contact Name	Sheriff Jeff Siegel
Contact Title	County Sheriff
Contact Phone Number	574-891-2300
email Address	jsiegel@elkhartcountysheriff.com
Facility Size	837
Date of Installation	Partner since 2003
Services	ITS, SVC, Tablets, IPRO, eMessaging, WordAlert

• CLIENT REFERENCE 2	
Facility Name	Dallas County, TX

<b>Contact Name</b>	Deputy Porfirio Limones
<b>Contact Title</b>	Deputy
<b>Contact Phone Number</b>	214-653-6679
<b>email Address</b>	Porfirio.Limones@dallascounty.org
<b>Facility Size</b>	6800
<b>Date of Installation</b>	Partner since 2005, tablet install 2021
<b>Services</b>	ITS, SVC, Tablets, IPRO, eMessaging

• CLIENT REFERENCE 3	
<b>Facility Name</b>	Montgomery County Texas,
<b>Contact Name</b>	Lt. Roland Henrici
<b>Contact Title</b>	Lieutenant
<b>Contact Phone Number</b>	936-760-5833
<b>email Address</b>	Roland.Henrici@mctx.org
<b>Facility Size</b>	938
<b>Date of Installation</b>	Partner since 1997
<b>Services</b>	ITS, Tablet, DMC, eMessaging, WordAlert

• CLIENT REFERENCE 4	
<b>Facility Name</b>	Leon Florida
<b>Contact Name</b>	Captain Georgella Dent
<b>Contact Title</b>	Captain
<b>Contact Phone Number</b>	850-606-3561
<b>email Address</b>	Dentg@leoncountyfl.gov
<b>Facility Size</b>	1150
<b>Date of Installation</b>	Partner since 2020
<b>Services</b>	ITS, SVC, Tablets, IPRO, STC, eMessaging, GEX, DMC

4. A disclosure of any personal or financial interest in any properties in the project area, or any real or potential conflicts of interest with members of the Sedgwick County Board of County Commissioners or county staff.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus does not have any personal or financial interest in any properties in the project area, or any real or potential conflicts of interest with the members of Sedgwick County Board of County Commissions or county Staff.

5. A description of the type of assistance, which will be sought from county staff, including assistance required from the county to lessen the costs of this project.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

No assistance is sought from Sedgwick County to lessen the costs of this project.

6. Provide documentation on all current and pending litigation.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to Attachment C to view the requested list of current and pending litigation.

7. Proof of insurance meeting minimum insurance requirements as designated herein.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to Attachment D for proof of insurance.

Securus Technologies does not maintain pollution liability insurance, as our operations do not involve activities that typically generate pollution risks. Our services primarily focus on technology solutions for secure communications and digital mail management, which do not include hazardous materials or environmental impacts that would necessitate such coverage.

We adhere to all applicable regulations and industry standards to ensure our operations are environmentally responsible and compliant. Should there be any specific concerns or requirements regarding environmental impact, we are happy to discuss our practices further. Securus can meet the insurance standards of the remaining items above.

8. Sample of software license agreement and sample of support agreement.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to Attachment E, for a sample of our Master Service Agreement (MSA).

9. Those responses that do not include all required forms/items may be deemed non-responsive.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

10. Non-Employee User Agreement.

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Please refer to Attachment F, for all required forms.

**11. Acknowledge receipt of Business Associate Addendum.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

Securus has reviewed each revision and addendum (a1 and a2) thoroughly and acknowledge receipt.

**12. Samples or images, including specification sheets, of proposed equipment must be provided.**

**SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY.**

All images and specification sheets are provided within proposal responses.

## IX. RESPONSE FORM

Response Form is located in Attachment F.