

PHONE SERVICE REQUIREMENTS

Respond to each of the items below:

1. **Vendor must provide outbound, collect person-to-person calling for intraLATA and interLATA services only. Acknowledge Vendor's acceptance of this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

2. **For Prisons (not work releases) - Blanket restrictions must be in place for operator and directory service numbers, 911 and other emergency service numbers, specific numbers such as the institution's employees, other long distance carriers via 950, toll free or by any other means. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus employs the most sophisticated intelligent validation network in the industry. As a real-time, computer telephony-based switching system, the Securus calling service never connects an incarcerant to a conventional dial tone. All dialed numbers—whether prepaid or collect—are thoroughly analyzed before the call is allowed to process. This includes determining if the area code and exchange are valid, checking the number against any restrictions such as customer requested blocks, confirming the payer has available funds or is credit worthy, and verifying through the national Line information Database (LIDB). The system will only dial a number after passing all of these tests.

Further, the NextGen Secure Communications Platform™ (NextGen SCP™) will allow authorized WA DOC personnel to put blanket restrictions in place for the all of the category of numbers listed in this requirement through the Global Call Blocking feature. This feature allows authorized facility personnel to manage blocked numbers using the platform user interface. Blocked numbers can be applied at various levels—facility, site, phone group, phone and incarcerant. NextGen SCP offers unlimited blocking so the resulting call blocking table that is created may contain as many entries as needed. In addition, there is an associated "Description" field that allows for additional information to be attached.

Typically, the call blocking list includes the phone numbers of local judges, sheriffs, facility personnel, jury members, attorneys and witnesses. This feature prevents incarcerants from making calls to the specific numbers listed in the table.

Securus will upload your call blocking list during the installation process to eliminate the burden of initial setup from your facility staff. All dial-around area codes and exchanges, such as 800, 900, and 976, are blocked by default. Access to live operator services, such as

0, 411, and 911, are also blocked by default. The call blocking list for work release sites can be configured differently to support the different rules at these sites.

Authorized users can search blocked numbers to see how the block is applied at the various levels. Results can be displayed by 25, 50, or 100 entries.

The screenshot shows the 'BLOCKED NUMBERS' interface in the Securus system. It includes a search bar with the text 'Search by blocked number or description' and a 'Search' button. Below the search bar, there are 14 results displayed in a table. The table has columns for Phone Number, Blocked Reason, Speed Dial, Description, Active, Location, and Site. The data is as follows:

Phone Number	Blocked Reason	Speed Dial	Description	Active	Location	Site
1 (214) 405-6239	Employee number		testash	✓	George Smith	Marketing Ne...
1 (214) 405-6239	Employee number		testash	✓	NG SCP Demo	All Sites
1 (214) 555-1212	Friend and...			✓	Helen IN Terminal...	EPMO Next G...
1 (214) 555-1212	Friend and...			✓	Sam Carver	Marketing Ne...
1 (214) 763-1880	Harras			✓	Marketing Next Gen...	Marketing Ne...
1 (214) 763-1880	Harras			✓	Helen in Terminal...	EPMO Next G...
1 (214) 763-1880	Harras			✓	Family Visitation	Marketing Ne...
1 (456) 865-4789	Harras			✓	Alex yyy Smithson	Marketing Ne...
1 (713) 555-1212	Witness number		Do not remove...	✓	Jimmy Jam Jones	Marketing Ne...
1 (817) 555-1212	Friend and...			✓	David L. McTier	Marketing Ne...
1 (817) 555-1212	Friend and...			✓	NG SCP Demo	All Sites
1 (972) 277-0321	Harras		Cool desk	✓	Hieronymus Bosch	EPMO Next G...
1 (972) 277-0321	Harras		Cool desk	✓	Marketing Next Gen...	Marketing Ne...
1 (972) 277-0415	Employee number			✓	Berry Greatness...	Marketing Ne...

3. All calls to 800, 900, 888 and other toll-free area codes must be prohibited unless explicitly permitted by DOC. The system must provide the ability to block and unblock certain area codes and numbers at will. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

During installing Securus will add all dial-around area codes and exchanges, such as 800, 900, 88 and 976, to the global block list so they are blocked by default. Access to live operator services, such as 0, 411, and 911, are also blocked by default.

It is possible to block and unblock certain area codes. Securus configures this capability into the facility's validation plan.

4. **The system must have the ability to limit the length of calls with varying length limits for different services. For example, the general rule is 20 minutes, but there are exceptions (e.g. suicide, OCO, VA numbers) which are limited to 90 minutes. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) has the capability to customize length of calls for different services or by PIN. The system can be configured to set the length of a standard incarcerant call to 20 minutes but also allow calls to special numbers to be set at 90 minutes, for example. These call limits are set at initial configuration of the system based on agency policy and can be changed or modified at any time with the appropriate system access credentials by staff or Securus support personnel.

In all instances, the system will give the incarcerant a verbal announcement one minute prior to end of their call and then enforces the facility policy with a hard stop.

5. **With the exception of ADA required communications (e.g. TTY/TDD, VRS, etc.) and except as otherwise identified by DOC, no live operators will be a part of the phone system. No access to human operators for directory assistance, long distance calls, caller assistance or any other reason will be permitted. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' standard configuration and technology underlying the NG SCP system does not allow access to outsider operators and instead uses connection to a private network to transfer and process incarcerant calls. When required, the system can be configured to allow access to specialize operators, such as those used to comply with ADA requirements.

Further NextGen SCP offers unlimited blocking through a call blocking table that can be used to prohibit access to a live operator for any type of calls. This feature prevents incarcerants from making calls to the specific numbers listed in the table. Securus will upload your call blocking list during the installation process to eliminate the burden of initial setup from your facility staff.

The call blocking table may contain as many entries as needed. In addition, there is an associated "Description" field that allows for additional information to be attached. Authorized facility personnel can manage blocked numbers using the platform user interface. Blocked numbers can be applied at various levels—facility, site, phone group, phone and incarcerant.

6. **All call attempts through any method (TTY/TDD, VRS, traditional phone, etc.), once cleared through the validation process, must include a recorded message to the call recipient including but not limited to the following:**
 - a. **Name and location of the originating facility.**
 - b. **Name of the calling party.**
 - c. **That the call is subject to monitoring and recording.**
 - d. **That any misuse may result in loss of telephone or visitation privileges, other violations, and criminal prosecution.**
 - e. **Instructions on how to accept or reject the call. Must require a key press to accept the call.**
 - f. **Menu of other options, i.e. cost of the call, how to block the call, number to call for inquiries, and an option to replay all options at the end.**

Acknowledge Vendor's acceptance of this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

All call attempts (traditional telephone, TTY/TDD, VRS) will include a message to the incarcerant and called party that the call is from a correctional facility and that it is being recorded and/or monitored. The call set up announcements are configurable. We will configure the NextGen SCP incarcerant calling platform to include all of the required statements listed in this requirement. Additionally, the called party will have the ability to decline the call and block the caller for future purposes, if desired.

The Securus calling service includes an Interactive Voice Response (IVR) system that provides Automated Operator Services (AOS). This automated assistance uses clear and concise, professionally recorded voice prompts to establish call acceptance and to assist incarcerants and called parties throughout the calling process.

When the called party answers the phone, the calling service's advanced answer detection triggers the call acceptance voice prompt. The called party hears, "Hello, you are receiving a collect call from [incarcerant's name], an incarcerant at the Washington Department of Corrections [name of facility and location]. This call is subject to monitoring and recording." SCP then gives the called party the following menu options:

- "To accept this call, press 1."
- "To refuse this call press 2."
- "To hear the rates and charges for this call, press 7."
- "To block future calls to your number, press 6."

Additional options provided by AOS include:

Available Options to Called Parties

- Request a rate quote
- Hear the name of the facility and incarcerant calling, ex. "Hello, you are receiving a collect call from [incarcerant's name], an incarcerant at the Washington Department of Corrections [name of facility and location]."
- Accept or reject the call
- Request available balance of an AdvanceConnect account or available credit of the Direct Bill account
- Hear instructions on how to add more money to their prepaid account or pay their Direct Bill Account
- Connect to a live agent to setup a pre-paid account
- Choose to hear the prompts on the system in English, or the language selected by the incarcerant (if configured for this option)
- Pay for the incoming call with InstantPay (if available)
- Hear optional marketing message (by request of Washington Department of Corrections)
- Block their number prior to accepting a call using the system's Perma Block technology*

Available Options to Incarcerants

- Listen to prerecorded announcements
- Choose to place a collect or debit call; if debit, PIN entry is requested, the incarcerant hears the available balance in their account and the cost of the call
- Select a specific language at the beginning of the call (if configured)
- Acknowledge that the call is going to be monitored and recorded
- Hear available call time (prompt will tell the incarcerant call time limits based on calling schedules or calling restrictions)
- Identify themselves by PIN or Voice Biometrics (if configured)
- Add, remove, and/or listen to the phone numbers on their PAN list (if configured)
- Hear optional marketing message (by request of Washington Department of Corrections)

***The calling service's automated operator also provides a Perma Block process, which allows a called party to block their number permanently. This feature may be used to block calls from any incarcerant in the facility. The ability to immediately block calls helps reduce the number of called party complaints. The called party can also choose to end the call by hanging up.**

TTY Devices

Whether it is the incarcerant that is hard of hearing or the called party, NG SCP Call prompts are displayed on the TTY device being used for the incarcerant and/or called party to read.

VRS Devices

Incarcerants using VRS will place their calls on the sPhone XL terminal with the ConnectUs operating systems. The ConnectUs software is intuitive, easy to use, and will guide the Offender through the calling process.

- **Call from Offender VRS Device to Called Party VRS Device** – When an Offender uses the ConnectUs VRS application to place a call to another VRS-capable phone, when the called party answers Purple communications will play a video recording announcing in American Sign Language (ASL) and with closed captioning that “this call is from a correctional facility. This call may be monitored.” This will be seen by both the Offender and called party.
- **Call from Offender VRS Device to Non-VRS number** – In this scenario, the VRS operator serving as the interpreter for the Offender will advise both the offender and the called party that the call is being recorded.

**7. The system must allow the recipient to decline the call after being presented with the above information. Describe how Vendor will meet this requirement.
Vendor’s response:**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The calling service’s automated operator provides the option to decline that specific call by pressing 2 or allows the called party to block their number permanently through the Perma Block process. This feature may be used to block calls from any incarcerant in the facility. The ability to immediately block calls helps reduce the number of called party complaints.

To automatically block the number, SCP gives the called party the following menu option:

- “To block future calls to your number, press 6.”

**8. Recordings/prompts must be customizable by DOC to permit different recordings per location at no cost to DOC. Describe how Vendor will meet this requirement.
Vendor’s response:**

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Recordings and prompts are customizable per WA DOC location at no cost to the DOC. During installation, our teams work with WA DOC personnel to provide the necessary recordings. We can modify the recordings at the WA DOC’s request and will do so at no cost.

The following tables provide examples of different calling options and the associated announcements that can be configured to meet your needs:

Incarcerant Calling Options

Incarcerant Chooses Collect Call Option

- "Please enter your PIN number now." (*repeated*)
- "Please enter the area code and telephone number you are calling now." (*repeated*)
- If voice biometrics is being used, "You will be asked to verify your voice now. Please say your name after the beep."
- If voice biometrics is being used, "Please say the facility name after the beep."
- "This call is subject to monitoring and recording. To continue, press 1. To disconnect, press 2."
- "You may hear silence during the acceptance of your call. Please continue to hold."

Incarcerant Chooses Debit Call Option

- "Please enter your PIN number now." (*repeated*)
- "You have (X) dollars and (X) cents."
- "Please enter the area code and telephone number you are calling now." (*repeated*)
- "This call will cost (X) dollars and (X) cents for the first minute and (X) dollars and (X) cents for each additional minute, plus any applicable telecom and sales taxes."
- If voice biometrics is being used, "You will be asked to verify your voice now. Please say your name after the beep."
- If voice biometrics is being used, "Please say the facility name after the beep."
- "This call is subject to monitoring and recording. To continue, press 1. To disconnect press 2."
- "You may hear silence during the acceptance of your call. Please continue to hold."

Specific Friends and Family Process

Friends and Family Receiving Call Process

Collect Call

"Hello. This is a collect call from (*Incarcerant Name*), an incarcerated at the Washington Department of Corrections. This call is subject to monitoring and recording."

- "To accept this collect call press 1. You may start your conversation now."
- "To refuse this collect call, press 2."
- "To prevent calls from this facility, press 6."
- "For a rate quote press 7."

Debit Call

"Hello. This is a debit call from (*Incarcerant Name*). An incarcerated at the Washington Department of Corrections. This call is subject to monitoring and recording."

- "To accept this debit call press 1. You may start your conversation now."
- "To refuse this debit call, press 2."
- "To prevent calls from this facility, press 6."
- "For a rate quote press 7."

Voice Overlays

Additionally, the NextGen Secure Communications Platform™ (NextGen SCP™) calling services allow voice overlay messages to be played throughout the call. These are also configurable and provide an additional fraud protection feature. An example of a voice overlay message is *"This call is from a correctional facility."*

Voice overlays can be configured to:

- Play the message randomly or a fixed number of times per call
- Set the number of times to play the message during the call
- Change the time between when the message plays and when to play the next message
- Set the delay between call acceptance and when to play the first message
- Set the amount of time before the end of the call to play the message

9. Following a notification of monitoring and recording, the system will require active call acceptance from the caller (e.g. pressing a button). Billing begins when the called party accepts the call. Acknowledge Vendor's acceptance of this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus acknowledges and accepts this requirement.

Billing for incarcerant calls begins upon positive acceptance of a call by the called party.

The Securus calling service requires active "called party" acceptance using touch-tones to complete calls. When the called party answers the phone, the calling service's answer detection triggers the call acceptance voice message. This message announces the incarcerant's call and asks the called party to accept or reject the charges of a collect call. The called party is instructed to dial a single digit on their telephone to accept the collect call charges, or hang-up to disconnect the call and refuse charges.

10. The system must provide the ability to establish a line credit per billed number. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus offers Family and Friends two types of payment/billing options - AdvanceConnect / Prepay and Direct Bill.

- **AdvanceConnect/Prepaid account:** Securus' AdvanceConnect payment product allows family members and friends to pre-pay for calls originating from incarcerated individuals in correctional facilities. AdvanceConnect is flexible in that it allows consumers to prepay for multiple calls or prepay for a single call just prior to connection using the AdvanceConnect Single Call feature. AdvanceConnect Single Call allows friends and family members to fund the bare minimum to complete the current inbound call.

Other Key Features of Securus Advance Connect

- **AutoPay:** AutoPay for AdvanceConnect allows consumers to fund their account automatically with a preset amount of their choice when their balance is low. They can subscribe to the program and receive notifications via email or text message.
- **TextPay:** a customer can register to receive a text notification that will give them the option to fund their AdvanceConnect account immediately with a preset amount of their choice by responding with the word PAY.

The Payor will receive a text notification with payment confirmation with both AutoPay and TextPay.

- **Direct-billed accounts by Securus:** Securus offers direct billing as an option to our end user customers. A direct-billed account allows collect calls to be billed monthly directly from Securus Correctional Billing Services. Family and friends then have 28 days from the invoice date to pay their direct bill. To set up a direct-billed account, the incarcerated individual's family member or friend provide Securus Correctional Billing Services with their billing telephone number, name, and address, and are subject to a credit check (as allowed by state regulations). Securus does not restrict its direct billed option to businesses and attorneys.

Other Key Features of Securus Direct Billed Accounts

- For accounts past due, calling to the billed number is blocked until the account is paid in full.
- Non-payment call block is removed immediately upon receipt of payment: Payment can be made at any time.
- Securus does not charge a non-refundable deposit or charge for an account that has not been paid within thirty (30) days of bill due date.
- Securus does not charge a bill processing fee for the monthly statement.
- Securus will convert Direct Billed accounts, 7 days past due, to AdvanceConnect / Prepay.

Account Activator

Securus completes as many calls as possible and provides the incarcerated individual with descriptive prompts as to why a call might be blocked. One of our initiatives for completing every call is our Account Activator application.

For calls to numbers that can't be billed with traditional collect billing methods, Account Activator allows a brief conversation to occur during the first call to that number and then requires the called party to set up an account to receive future calls.

After the brief conversation, the incarcerant's friend or family member is connected to Securus' IVR in an attempt to set up a billing arrangement. During this time, the incarcerant is informed of the blocked status and requested to call at a later time while an account is set up for the called party.

- 11. The system must utilize a personal identification number (PIN) to identify each incarcerant caller by DOC number and reference a list of permitted numbers that the incarcerant may call. Modifications to the list of permitted numbers must be limited (number and frequency to be decided by DOC). Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With Securus' NextGen Secure Communications Platform™ (NextGen SCP™), each incarcerant telephone is individually programmed for Personal Identification Number (PIN) or non-PIN operation. This provides maximum flexibility in PIN placements. For example, a facility may wish to allow PIN operation in maximum security or long-term areas, while allowing an "all calls" option in overnight, work release, or trustee areas. The calling service has no limit or restrictions on the number of PIN or non-PIN incarcerant telephones operating at the facility.

Some facilities may choose to assign each incarcerant a unique PIN that they must enter before making a telephone call. PINs also provide an audit trail of the incarcerant who placed each specific call. PINs also allow the facility increased control over which incarcerants can call which numbers.

Each incarcerant is assigned a unique PIN, ranging anywhere from 4 to 16 digits. This range creates a maximum number of 9 billion PIN combinations.

Facilities can choose one of the following three primary modes to a single phone or group of phones in a facility:

- Mode 1, Open PIN
- Mode 1, Open PIN with Restrictions
- Mode 3, Closed PIN

Mode 1, Open PIN

This is the most basic mode of operations, and the simplest to administer. Each incarcerant is assigned a unique PIN to make a phone call. There are no individual phone number restrictions or calling lists in this mode. NextGen SCP applies global system calling restrictions to every call.

Mode 2, Open PIN with Restrictions

Mode 2 builds on the Mode 1 Open PIN feature and adds the ability to place call restrictions and limits on specific call types while allowing all other phone numbers to process as they would in an Open PIN system. Mode 2 restrictions can include the recording and alarming of numbers and the use of the facility or global number lists for special circumstance numbers, such as attorneys and external crime tip numbers.

Mode 3, Closed PIN

Mode 3 provides the most restrictive calling privileges. It also requires the most administration of the three modes. Each incarcerant registers telephone numbers on their personal allowed number (Pan) list. The total number of destination numbers available is unlimited. The facility determines the maximum number of telephone numbers each incarcerant can register. Telephone number registration includes the number, name of the called party, and their relationship to the incarcerant. The telephone numbers that each incarcerant registers are associated with the incarcerant's PIN and reside in the system. Only that PIN may validate calls to those numbers. Updating calling lists is a continuous process as incarcerants are booked into, or released from the facility, or as the incarcerants request changes to their calling lists. This type of control is usually recommended only for facilities with a low rate of incarcerant population turnover, or where such extreme security measures are desirable. Note that in a Closed PIN environment, the facility may choose to make certain telephone numbers commonly available to all incarcerants. The common numbers may be assigned global or facility accounts.

Securus provides an automated PIN and PAN management system called E-Imports that can off-load facility labor required to enter PINs and PANs manually.

At initial installation, Securus will request the current PAN list from your current provider and enter the data into our NextGen SCP so that upon cutover to the system, incarcerants will have the same dialing privileges; or restrictions, that currently exist.

Personal Allowed Number List

The Personal Allowed Number (PAN) feature in the NextGen Secure Communications Platform™ (NextGen SCP™) provides an approved calling list for each incarcerant. Authorized WA DOC users can add both allowed and blocked numbers to the PAN list.

Please consider that Securus believes that with new investigative tools now available to agencies and the ability to notify investigators when calls are made to specific numbers combined with new incarcerant to incarcerant call detection, PAN lists are unnecessary and carry a difficult administrative challenge. However, if the agency would like to continue the use of PAN's to restrict incarcerant calling, Securus can assist with the administrative

requirements by deploying a site administrator to offload staff from PAN administration duties.

Securus built this feature with the awareness that each facility has unique needs for implementing allowed calling lists. Like all other features of NextGen SCP, the PAN lists can be administered manually, automatically, or by importing through E-Imports. The PAN configuration options include:

- **Auto Pan:** Allows the first “X” numbers (defined by WA DOC) to be added to the incarcerant’s PAN list automatically. The quantity of numbers allowed is configurable.
This is the most popular method of PAN administration. Numbers are loaded immediately without the intervention of staff, maximizing revenue potential.
- **Incarcerant Managed PAN:** Allows incarcerants to manage their list, including adding a new number, removing a number, checking the status of a phone number, or hearing the phone numbers on their list. When an incarcerant adds a phone number to their list, the automated system conducts a real time billing name and address (BNA) lookup on the phone number. If NextGen SCP finds a valid BNA, it will call the phone number and ask the called party to accept being on the specific incarcerant’s PAN list. No staff time is required to administer this process. With the extra step of validation, the DOC has maximum control of each added number.
- **Manual PAN Entry:** Authorized facility personnel can accept calling lists from incarcerants, verify the phone numbers, and enter them into the calling services user interface. This form of PAN administration allows a hands-on approach to approval and control of each number added to an incarcerant’s allowed number list.
- **PANs by System Integration:** NextGen SCP allows for the importing of PAN through our E-Imports application to add, create relationships, and deactivate numbers. There is no staff time required to administer this process. This is a specialized form of PAN administration, based on specific integration requirements of a facility.

Additional PAN Features

NextGen SCP provides administrators additional features to maximize efficiency, control, and inspection of PAN lists:

- Global Allowed List
- Automated List Refresh
- Verified/Not Verified PAN
- Speed Dial for PANs
- Associate PANs to PINs
- PAN Management Report

- PAN Change Log Report
- PAN Frequency Report

The following table provides descriptions of each PAN features and their primary benefit to WA DOC

PAN Feature	Primary Benefit	Description
Global Allowed List	Efficiency	Certain phone numbers, such as attorney numbers, can be authorized for all incarcerants by including them on the calling services “global allowed list.”
Automated List Refresh	Efficiency	With this automated feature, PAN lists can be configured to refresh every month on a certain day, such as the first of every month.
Verified/ Not Verified PAN	Safety and control	This feature flags numbers added to the incarcerant’s PAN list as “verified” or “not verified.” If the PAN is “not verified”, the incarcerant can call the number for a configurable number of days before it is blocked. Once the threshold number is reached and the number is blocked, a facility administrator must verify the number and if appropriate, allow calls to that number again.
Speed Dial for PANs		
Associate PANs to PINs		
PAN Management Report		
PAN Change Log Report	Safety and control	PAN Change Log functionality records all actions that NextGen SCP users make to the verified field in the calling services user interface. Allows administrators to examine all PAN list changes—specifically, when changes occur, and by whom, helping administrators and investigators track user accountability.

PAN Frequency Report

Safety and control

Shows phone numbers that appear in multiple PAN lists. Users can enter threshold numbers to define search criteria. For example, a threshold of "four" will show phone numbers that appear in PAN lists more than four times. This report also allows users to create a detail report with specific detail for each call.

12. The system must have redundancy of switching equipment. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Redundancy is a key component of the NextGen Secure Communications Platform™ (NextGen SCP™). While operating on a single platform, Securus' NextGen SCP runs on duplicate environments in separate data centers in Atlanta, Georgia, and Dallas, Texas. Each component has N+1 redundancy, meaning that a failure of any one component does not result in downtime because there is a backup available to resume its function. In addition to the inherent redundancy of NextGen SCP, Securus has also designed redundancy into all support systems, either through N+ 1 configuration, database clusters, virtual machines, load balancing, or other failover methods. All network transport has redundant network equipment and routing to allow traffic to reroute in the event of a failure.

The NextGen SCP platforms in Dallas and Atlanta were designed and built to the same specifications. This standardization allows re-homing of systems from their primary data center to an alternate data center in the event of a failure.

All circuits coming into Securus data centers use multiple diverse carriers, including the interconnections between data centers. In the event of a failure, traffic will reroute across a redundant circuit or path. In addition, Securus uses multiple carriers for incarcerated calls from the NextGen SCP platform. Calls to family and friends will immediately reroute upon failure of any carrier.

Securus uses multiple methods of storage to minimize the risk of data loss. All critical systems and data are backed up at regularly scheduled intervals and stored offsite for retrieval, if needed. In addition to offsite storage, Securus replicates voice clips, call recordings, and validation data between the data centers.

Securus uses industry-leading vendors for all platform and network hardware, including Dell, Cisco, Oracle, EMC, Big IP, and Intel. In addition to the redundancy designed into the platform and network, Securus also maintains a spare parts inventory onsite at each of our data centers to expedite repair of a failed component. Securus also maintains premium-level support contracts with each vendor that define stringent service level agreements in case of a failure.

13. The system must provide a redundant call validation on a real-time basis allowing a maximum of 10 seconds for validation to eliminate access to blocked numbers, pay telephones or other non-billable numbers, using either a secure network, internet, or VPN, and, only as a backup validation method, dial-up. Describe how Vendor will meet this requirement.

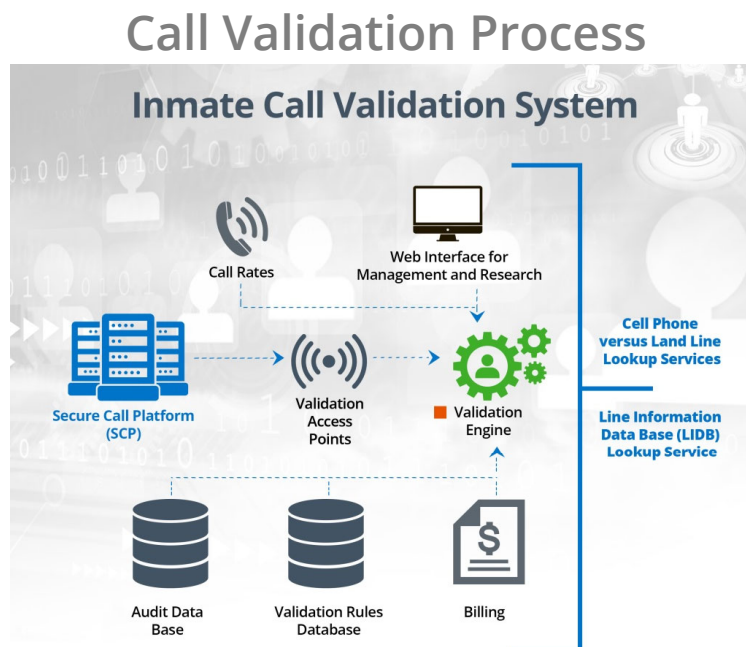
Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As a real-time, computer telephony-based switching system, the Securus calling service never connects an incarcerated to a conventional dial tone. Validation occurs in real time, not by batch. All dialed numbers—whether prepaid or collect—are thoroughly analyzed before the call is allowed to process. This includes determining if the area code and exchange are valid, checking the number against any restrictions such as customer requested blocks, confirming the payer has available funds or is credit worthy, and verifying through the national Line information Database (LIDB). The system will only dial a number after passing all of these tests.

Validation Process

We screen all calls to eliminate fraudulent activity, and to ensure only authorized individuals receive calls. The real-time validation process, as shown in the following graphic, outlines the elimination of unauthorized activity.



BUSINESS RULES

- Local Exchange Carrier (LEC) Billing relationship
- Billing Arrangements
- Inmate Restrictions
- Phone number Restrictions
- Cell Phone Allow / Deny
- Payment Funded Availability
- Facility Restrictions
- Global Dialing Plan and Restrictions
- Promotion Eligibility
- Available Talk Time
- Audit Logging

The following checks are performed during the validation process:

- If the facility uses personal allowed number (PAN) lists, the first check ensures that the number dialed is on the incarcerated's PAN list.
- All calls are verified to determine if the payer has requested a block.
- All calls are compared to system and administration blocks to ensure that un-allowed numbers are not called
- All collect calls are validated through AT&T's line information database (LIDB) to determine if the number has calling restrictions.

14. The system must provide an accurate name and billing address associated with the telephone number called. Describe how Vendor will meet this requirement:

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

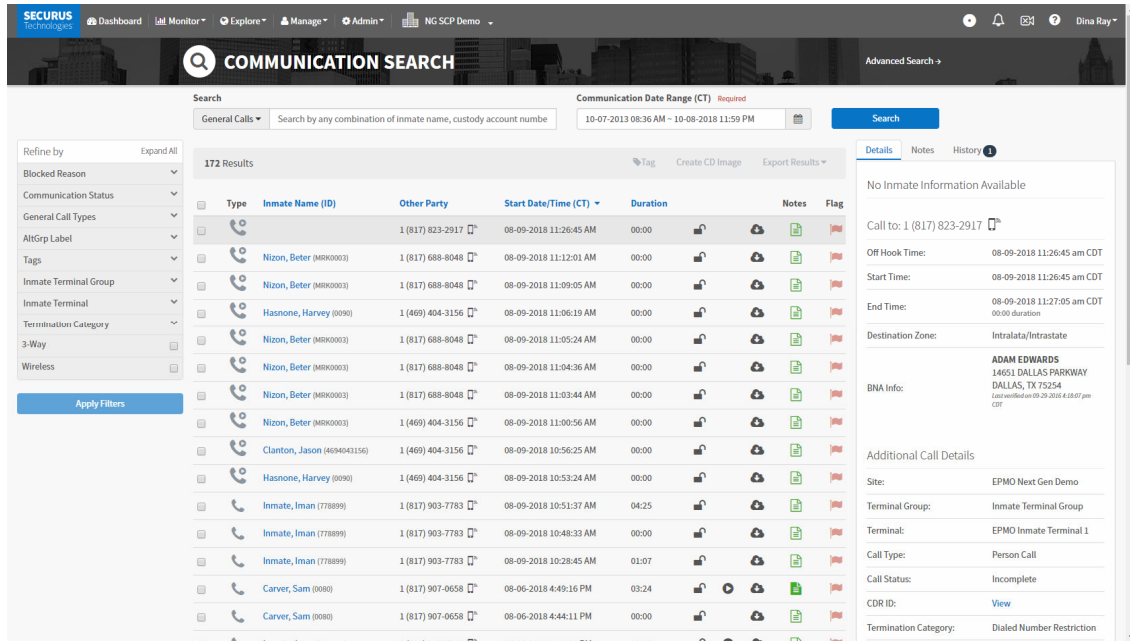
The NextGen SCP™ reverse lookup feature identifies the billing name and address (BNA) of a dialed phone number captured in a communication detail record (CDR). The system automatically shows this information, if known, in the Details panel. This search process is unique in the industry, providing the most accurate BNA information possible.

Authorized WA DOC users select a CDR and the BNA information, if available, appears in the side bar on the right-hand side of the page. The information includes the phone number owner's billing name, billing address, and the date the number was last verified. Unlike other similar tools in the industry today, Securus' fully-integrated reverse lookup feature is provided at no additional cost.

Reverse lookup, which is also available as a dashboard widget, allows users to access results from anywhere the number exists in NextGen SCP such as:

- Communication detail reports
- Blocked number lists
- Global allowed lists
- Call frequency reports

Dedicated BNA Search Screen



Reverse Lookup and Personal Allowed Numbers (PAN)

If using PAN management, NextGen SCP allows authorized users to associate the BNA information to a phone number on the PAN list. This feature allows administrators and investigative staff to view BNA information without an additional search. The Securus reverse lookup feature offers a comprehensive ad hoc search tool giving an authorized user the ability to enter criteria ranging from first name, last name, address, city, state, and ZIP to obtain this information on demand.

- The system must provide the ability for incarcerants to monitor their phone account information either through tablet, kiosk or specific service number on the system. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus' communications solution will allow the incarcerant to monitor their phone account information through our Automated Information Services (AIS) and through the ConnectUs terminal.

Automated Information Services

Securus' Automated Information Services (AIS) is the most comprehensive IVR in the industry which provides general facility and incarcerant-specific information to detainees over the phone. To access AIS, incarcerants dial a speed-dial code from any incarcerant telephone and they will be provided with various information including:

- Incarcerant Debit balance
- Criminal charges
- Bond amounts and types
- Court dates, times, and locations
- Projected release date
- Commissary balance
- General facility information
 - Facility location
 - Directions
 - Hours
 - Mailing policies
 - Visitation policies
 - Money deposit policies

All functionality is available around the clock, allowing incarcerants to access the system whenever they need it.

AIS retrieves information from a facility's various management information systems, including offender management and court systems, every 15 minutes. The service offers an English and Spanish interface, text-to-speech playback of incarcerant names, and a touchtone and speech recognition interface.

Incarcerant Information through ConnectUs

ConnectUs terminals can be set to require Incarcerant Login. Incarcerant Login gives an incarcerant the ability to create his own personal account to a self-service portal. The feature provides the incarcerant access to his information, services and applications with a single sign-on. The incarcerant will now be able to manage and view his authentications, logins, and activities within the configured applications and systems accessible by a terminal.

Once the incarcerant has logged into the ConnectUs terminal they will be presented with access to:

- Account Information – Shows key account information and allows incarcerant to update his photo and password
- Activities – Shows most recent logins, calls and visitations
- Financial Information – Shows debit call balance



- 16. The DOC bears no responsibility for the loss of revenue as a result of fraudulent use of the telephone service. Vendor will work to minimize fraud. Acknowledge Vendor's acceptance of this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Fraudulent calls are calls where end user intends to defraud, deceive, or cheat, usually for the purposes of causing financial loss to another, or bringing financial gain to oneself. We use our best efforts to prevent fraudulent calls but, when they do occur and are reported to us by the end user who receives the call, we will provide a credit to the end user's account for the call. In no event will the DOC have responsibility for our loss of revenue in these situations.

- 17. The phone system must provide voice prompts in both English and Spanish. Acknowledge Vendor's acceptance of this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus automated operator uses clear, concise, professionally recorded voice prompts to assist the incarcerant through the calling process. By default, the Securus calling service offers language prompts in both English and Spanish. Securus can provide additional languages on request. Calling services can be configured to provide prompts in as many as nine languages.

Some examples of languages that Securus has implemented in the past include:

Afrikaans
Arabic

Hebrew
Hindi

Slovak
Slovene

Bahasa	Hungarian	Somali
Bulgarian	Icelandic	Spanish (U.S., Mexico, Puerto Rico, Central and South America, Castilian dialects)
Chinese (all dialects)	Italian	
Creole/Haitian	Japanese	
Croatian	Javanese	Swedish
Czech	Kannada	Tagalog
Danish	Korean	Taiwanese
Dutch	Latvian	Tamil
Estonian	Lithuanian	Telugu
Finnish	Malay/Malayalam	Portuguese (Brazil and Portugal dialects)
Flemish	Marathi	
French (Canadian and Parisian dialects)	Norwegian	Turkish
	Polish	Urdu
German/Bavarian	Punjabi	Ukrainian
Greek	Romanian	Vietnamese
Gujarati	Russian	

After the language prompts are set up in the calling service system, incarcerants select their language choice at the beginning of the call process by dialing a single digit.

During call acceptance, the called party receives the acceptance instructions in English first followed by an option to continue in the language selected by the incarcerant. This fraud deterrent feature eliminates incarcerant attempts to confuse called parties with a language they do not understand.

- 18. The system must provide a 1-minute notice to incarcerants when their call time is about to expire. Additional prompts must be available at Department's discretion. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus call termination warning provides the incarcerant and the called party notifications of call termination by voice prompt one minute before the end of the pre-programmed call time limit.

Additionally, the NextGen SCP™ calling service allows voice overlay messages throughout the call as an additional fraud protection feature. An example of a voice overlay message is *"This call is from a correctional facility."*

Voice overlays can be configured to:

- Play the message randomly or a fixed number of times per call
- Set the number of times to play the message during the call
- Change the time between when the message plays and when to play the next message
- Set the delay between call acceptance and when to play the first message
- Set the amount of time before the end of the call to play the message

19. All telephone lines installed must be able to provide simultaneous service at all times, with no limitations due to provider equipment and services. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will maintain sufficient capacity and bandwidth to provide a user experience with minimal buffering or delay for all services Securus offers at WA DOC facilities. Our service quality meets or exceeds all current industry standards.

Line Capacity

The system and network maintain twice the capacity of normal calling volume to prevent blocking of outbound calls and busy signals. The central processing system and its network capacity can scale to many times their current capacity within the current architecture and design.

Securus monitors the system 24x7x365. When concurrent telephone call volumes reach a predetermined threshold (not at the limit), additional capacity is added. Since the system capacity is managed to keep ahead of call growth, the maximum number of incarcerant phones is limited only by the connectivity delivered to the facility.

Bandwidth

We dedicate enough bandwidth for each conversation over our private network to keep packet delays under 100 milliseconds which provides the ability to achieve an MOS of 4.3 (better than digitized telephone quality). Further, we use a mixture of G.711 and G.729a signaling protocol.

Securus adds additional circuit bandwidth to each site and the central data center when necessary.

20. **The system must be scalable to any new facility/new construction and/or expansion or upgrade of current facilities. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our proposed equipment and system is scalable to meet WA DOC's growing needs.

Scalability of NG SCP Central Processing System and Network

The NG SCP is a centralized call management system and network that maintains twice the capacity of normal calling volume to prevent blocking of outbound calls and busy signals.

The central processing system and its network capacity can scale to many times their current capacity within the current architecture and design. Securus monitors system 24 hours per day, seven days per week, every day of the year. When concurrent telephone call volumes consistently cross 80% of the available capacity, additional infrastructure is added to our central processing system to augment the capacity. Since the system capacity is managed to keep ahead of call growth, the maximum number of incarcerant phones is limited only by the connectivity delivered to the facility. Securus adds additional circuit bandwidth to each site and the central data center when necessary.

Our SCP uses private Multi-Protocol Label Switching (MPLS) circuits within our network. MPLS is widely accepted to be the premium service available for transporting digitized voice signals. Further, we use a mixture of G.711 and G.729a signaling protocol and we dedicate enough bandwidth for each conversation over our private network to keep packet delays under 100 milliseconds which provides the ability to achieve an 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.

Scalability of Storage

Securus stores call recordings in centralized, disaster-resistant, carrier-class data centers. All equipment used to store recordings is monitored by the Securus Network Operations Center (NOC) 24 hours a day, seven days a week, and 365 days a year.

The Securus data center storage solutions provide facilities with technology that is:

- **Scalable** to meet any facility's contractually required storage demands
- **Resistant** to local disasters through multiple copies stored within the data centers and off-site
- **Highly available** through the unique architecture and design of the data storage model
- **Partitioned and compressed** to run queries faster
- **Secure, protected, and monitored** to enable total recall of data

The NAS architecture makes all storage available to all servers on the network. The 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. The NAS devices provided by EMC can scale simply by adding another node of dense SATA disk to the storage array. Within the NAS, SCP uses a software defined storage platform of very dense disk nodes. Even if three individual hard disk drives fail or one node fails, during the disk or node recovery process, the system will continue to operate without data loss.

The Securus NAS has more than seven petabytes of storage space in each carrier-class data center and is continuously monitored and managed through automated processes and storage policies. When these very large storage systems approach designated thresholds, Securus expands capacity to ensure all authorized call records and recordings are retained in secure, disaster-resistant locations.

Scalability of Equipment

If WA DOC requires additional equipment, the DOC can coordinate with its assigned Account Manager. Additionally, Account Management will routinely evaluate the needs of the DOC and propose solutions to make sure we keep WA DOC functioning at the highest capacity.

21. The hours of operation for the phone system must have the ability to be set by facility and by housing unit. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The NextGen Secure Communications Platform™ (NextGen SCP™) calling services has automated calling schedules that allow the system to enforce the scheduling policies of the facility without staff intervention. Calling schedules are used to turn on and off the phones during designated times throughout the day or night.

Calling schedules are flexible and configurable allowing the facility to have multiple on and off times during the day, within a week and by day of the week and then be applied to individual telephones, groups of telephones, individual incarcerants and/or globally.

Also, holiday overrides can be preset to accommodate anticipated exceptions to the set schedule.

Programming Calling Schedules

The screenshot shows the 'CREATE CALL SCHEDULE' interface. At the top, there is a navigation bar with 'SECURUS Technologies' and various menu items like 'Dashboard', 'Monitor', 'Explore', 'Investigate', 'Manage', and 'Admin'. The main header reads 'CREATE CALL SCHEDULE' with 'Cancel' and 'Save' buttons. The form is divided into sections:

- Call schedule details:** Includes a 'Call Schedule Name' field (marked 'Required') with a callout 'Create a call schedule name.' and a 'Disconnect rule' section with two radio buttons: 'Allow in progress calls to finish when scheduled time ends' (selected) and 'Terminate calls immediately when scheduled time ends'. A callout 'Select the appropriate disconnect rule.' points to these options.
- Call schedule settings (CDT):** Includes a note 'Overlapping events on the same day will be treated as one continuous event.' and a 'Schedule locations' link. Below is a calendar grid with columns for days of the week and rows for times from 12:00 am to 6:00 am. A callout 'Click the days and times on the calendar to set the on/off times.' points to the grid.
- Holiday Exceptions:** Includes an 'Add Exception' button and the text 'No holiday exceptions have been added.' A callout 'Add a holiday exception,' points to the button.

At the bottom, there are 'Cancel' and 'Save' buttons.

Programmable calling schedules are responsive to and overridden by both the manual cut-off switches located within the facility and the Call Settings Disconnect Rule.

- 22. The phone system must have the ability to apply call restrictions per housing unit / per incarcerant / per telephone number. Describe how Vendor will meet this requirement.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

As incarcerant phones are a shared resource, facilities often need to enforce the equitable sharing of them. WA DOC may use call restrictions to regulate incarcerant access to phone to ensure access by all incarcerants.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides calling restrictions to give WA DOC control of calling activity at the incarcerant, port, phone group, facility, or customer level. Multiple restrictions can be crafted within each restriction set.

Examples of call restrictions are:

- Maximum number of calls per day/week/month
- Maximum type of calls per day/week/month
- Maximum number of call connects, accepts and/or mins of talk time

All imposed calling restrictions are automatically managed by the NextGen SCP system to relieve facility staff of calling restriction enforcement responsibilities.

Restrictions may also be used for punitive measures or behavior modification by restricting access versus revoking complete access as done through suspension.

WA DOC personnel may shut off access to any particular phone, group of phones, facility, or the entire DOC if necessary at any time through electronically through NextGen SCP. In addition, during installation we can installed emergency manual shut-off switches at DOC facilities should the DOC so desire

23. The system must provide DOC the ability to shut off any or all phones through software application and/or hardware switches. Describe how Vendor will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The Securus NextGen Secure Communications Platform™ (NextGen SCP™) provides complete flexibility to disable telephone use at any time of day through manual intervention or preset calling schedules.

NextGen SCP allows authorized users to disable a telephone, group of telephones, or all facility phones using any personal computer with access to the Internet. This capability is available anytime, from anywhere, 24x7x365.

This function allows authorized users to kill all calls immediately or allow current calls to finish while not allowing any new calls.

Disabling Telephones

Terminal: LP 10

Facility: Securus Demo Site
Site: Kellway Test Lab Allen
Terminal Group: BPA
Terminal: LP 10

Call Settings Covert Alerts 1

Terminal Status

Enable

Disconnect rule

Allow in progress calls to finish
 Terminate calls immediately

Terminal Settings

3-Way Calling Detection
Value set at: BPA. Override.

Voice Biometrics
Remove override and use setting from: BPA.

Uncheck "Enable" to disconnect all calls.

Select the appropriate disconnect rule to terminate all calls immediately or allow in-progress calls to finish.

Calls can be terminated by site, terminal group, or individual terminals.

Save

In addition, during installation can install emergency manual shut-off switches at DOC facilities should the DOC so desire.

24. Telephone support must be available to accept calls from incarcerants and friends and families regarding customer service, billing, prepaid account setup, technical, and funding issues. Incarcerants should be able to access phone account information and phone customer service on their tablet or via kiosk. Describe how you will meet this requirement including your customer service hours.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus is unique among its national competitors in offering an in-sourced, US-based call center (Securus Friends and Family Call Center, SFFCC) to provide customer service to friends and family members of incarcerants. Our 200+ seat call center employs customer service representatives who are Securus employees, trained and managed to Securus' standards.

Live agent support is available to friends and family members seven days a week, 24 hours a day, and 365 days a year.

Securus will set up a separate dedicated toll-free number just for WA DOC friends and family to contact customer service. Customers can also use our general toll-free number (1-800-844-6591) to either speak to a live agent or use an intuitive, automated interactive voice response system to help them with their needs. For added convenience, we also offer personal account access via our website (www.securustechnologies.com). End-users can also now access SFFCC via online "chat" 24 hours a day, seven days a week.

Our friendly and knowledgeable agents can help customers with:

- Setting up and funding accounts
- Making payment arrangements
- Obtaining information on credit limits
- Resolving complaints
- Blocking and unblocking numbers
- Reviewing call durations and history
- Learning about MoneyGram® options
- Learning about Western Union® options
- Receiving information on new services
- Confirming originating facility
- Reviewing account balances
- Answering questions and helping customers with refund requests
- Managing account notifications

Our customer service agents are highly trained on ITS issues and in satisfying the specific needs of called parties. We offer both English speaking and Spanish speaking agents.

We diligently survey our customers and measure satisfaction ratings to find ways to improve our service levels. Our customer satisfaction scores for our call center are 20 percent higher than the industry standard.\

Securus strives to deliver superior customer service and resolve customer issues in one call. Securus Friends and Family Call Center (SFFCC) supervisors are always available to assist customers when an issue requires escalation. Some issues may require time to research and resolve. For all issues, the following escalation list may be utilized after 24 hours:

- Escalate to customer service manager;
- If still unresolved, escalate to the director of customer care;
- If still unresolved, escalate to vice president of customer care.

Incarcerant Technical Support

Securus can provide a pre-arranged speed dial number where the incarcerant can leave a message for support regarding customer service, billing, prepaid account setup, technical, and funding issues.

The NextGen Secure Communications Platform™ (NextGen SCP™) allows the DOC to create speed dial numbers that allow incarcerants to use shorter numbers, such as “101” or “111,” for dialing important numbers, such as incarcerants services, medical alerts, officer assistance, TTY, information, commissary, or emergency lines.

The calling services allows speed dial numbers to be crafted using 3 to 10 digits and provides the DOC with a virtually unlimited set of programmable speed dial numbers.

Further, for calls received at this line there is:

- An option to burn specific information onto CDs for use as evidence
- A way to generate reports of all recorded messages with the date and time of the message
- A way to leave a reply message to the incarcerant

Submitting a Service Request through the Incarcerant Kiosk

In addition to the speed dial number that will be created for incarcerants to make service requests, the current system of submitting a request through the Communication Center on the kiosk will also be available. Originally designed to solve an agency's need for incarcerants to be able to file complaints and grievances, the Communication Center is available for incarcerants to submit various types of forms and support tickets through the kiosk or through the application on a tablet device.

Making submission of service requests a digital process reduces the amount of paper forms and simplifies the process so that all communications can be tracked and audited. The Communication Center allows incarcerants to submit and maintain a back and forth conversation as needed with facility staff and our Inmate Support team. Incarcerants are able to send support tickets covering a multitude of topics in order to request assistance from our Inmate Support team (as shown below).

The screenshot shows the JPay kiosk interface. At the top, a blue header bar displays the JPay logo, the text "Welcome STEPHEN SMITH", and the time "11:22 AM". Below the header is a navigation bar with buttons for "Back", "Home", "Help", "FAQ", and "Log Off". The main content area is titled "Start a New Communication". It features a "Form" dropdown menu set to "JPay Support Ticket", a "Subject" dropdown menu with a list of options including "Accessories", "Banking", "Games", "Player", "Kiosk", "Mail", "Music", "Video Visitation", "VideoGram", "KA Lite", "Video Store", and "Battery", and a "Description" text area with a "3200 character(s) left" indicator. At the bottom of the form are "Cancel" and "Continue" buttons. The footer of the kiosk displays "Kiosk Online Kiosk ID: AHCC022", "Session Time Left: 17:52 minutes", and "Stamp(s): 193".

Incarcerant Information through the ConnectUs Terminal

ConnectUs terminals can be set to require Incarcerant Login. Incarcerant Login gives an incarcerated the ability to create his own personal account to a self-service portal. The feature provides the incarcerated access to his information, services and applications with a single sign-on. The incarcerated will now be able to manage and view his authentications, logins, and activities within the configured applications and systems accessible by a terminal.

Once the incarcerated has logged into the ConnectUs terminal they will be presented with access to:

- Account Information – Shows key account information and allows incarcerated to update his photo and password
- Activities – Shows most recent logins, calls and visitations
- Financial Information – Shows debit call balance



25. Describe your support for reports of phone hardware issues. Include in your description how you determine the priority levels for phone issues, as well as expectations regarding timelines. Also include how you will track phone issues and report these issues to the DOC contract manager.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus provides superior customer service from a state-of-the-art operations center located on the first floor of our headquarters billing in Carrollton, Texas. More than 50 technicians staff the Securus Technical Support Center (TSC) to ensure prompt problem

resolution. The average tenure of our technicians is 8 years and the average tenure for our technical support management is 10 years.

The Securus TSC serves as a single point of contact for facility staff to request service **24 hours a day, seven days a week, 365 days per year**. There are three ways to contact the TSC:

- Telephone: 866-558-2323
- E-Mail: technicalsupport@securustech.net
- Fax: 800-368-3168

The technical service center offers our clients:

- Technical support and field dispatch 24x7x365
- Fully trained staff of support professionals to answer calls
- Trained professionals to provide quick problem resolution and a higher level of customer service
- Service event tracking to drive resolutions
- Prioritized calls and analyzed reports to ensure achievement of Service Level Agreements
- Certified technicians to provide quick problem resolution
- System and individual site connectivity monitored 24x7x365

The TSC uses a call distribution system to manage the flow of inbound customer calls automatically routing calls directly to our support technicians in a skills-based, platform specific manner. Securus will establish a dedicated toll free number for the Washington DOC facility contact with Securus Technical Support. Securus establishes response times and service level agreements that accomplish our objective of providing timely resolution to each request.

Technicians assign each service request one of three initial priority levels, each with resolution and escalation timelines that will be consistent with the service level agreement between the Washington DOC and Securus. Every effort is made to resolve the problem remotely within the designated timeframes, and Securus resolves most service requests during the initial request. If necessary, a field service technician is dispatched to the facility to expedite resolution.

The TSC uses an event tracking system that logs, tracks, manages and assures appropriate response to all service requests. The service request generates a trouble ticket with priority level assignment that drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem and either resolves the problem or engages an appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

Service Response Times and Escalations

Priority Level	Service Priority Description	Response Time	Customer Communication Guideline	Escalations
P1	A P1 is our highest service level defined as 30% or more of the functionality of the System being adversely affected by the System Event. Examples of P1 service assignments would include items such as no voice prompts, features not operating appropriately, inability to burn CD's, issues with listening to live calls, inability to access NextGen Secure Communications Platform™ UI, all phones down.	2 hours	<ul style="list-style-type: none"> Securus Technical Support Center notifies the facility when the service issue is resolved If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival 	<ul style="list-style-type: none"> If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request Technical Support Manager & Field Service Manager Technical Support Director & Field Service Director VP Service & Operations
P2	A P2 assignment defined as 5% to 29% of the functionality of the System being adversely affected by the System Event. Examples of a P2 service assignments would include items such as workstation, specific system ports, LEC circuits, unblocks, block numbers, missing CDRs, call searching.	24 hours	<ul style="list-style-type: none"> Securus Technical Support Center notifies the facility when the service issue is resolved If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival 	<ul style="list-style-type: none"> If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request Technical Support Manager & Field Service Manager Technical Support Director & Field Service Director VP Service & Operations
P3	A P3 assignment defined as less the 5% of the functionality of the System	72 hours	<ul style="list-style-type: none"> Securus Technical Support 	<ul style="list-style-type: none"> If response is delayed, escalation procedures within

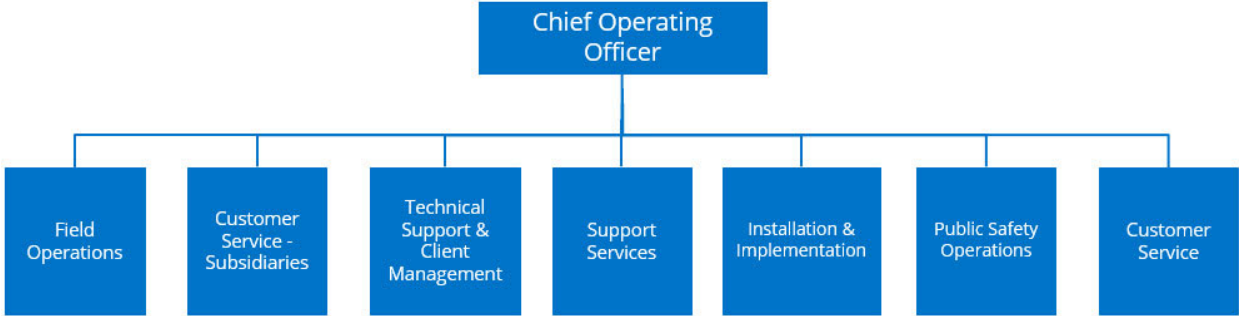
<p>being adversely affected by the System Event. Single and multiple phones related issues. Examples of P3 service assignments would include items such as static on the phone, a party not being able to hear, unable to dial, a broken phone, dial pad not working, cutoff switches not working, and inability to generate reports.</p>		<p>Center notifies the facility when the service issue is resolved</p> <ul style="list-style-type: none"> • If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival 	<p>Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request</p> <ul style="list-style-type: none"> • Technical Support Manager & Field Service Manager • Technical Support Director & Field Service Director • VP Service & Operations
---	--	--	--

Centralized Services Operations Model

All Securus services and operations are managed centrally, from our Service and Operations organization in Dallas, Texas. The Operations team's responsibility is supporting external customers, including Customer Service, Field Services, Installation and Engineering, and Technical Support. The Support Services team provides internal support services including Quality, Training and Customer Satisfaction, and Reporting and Analysis.

The following figure illustrates the Securus Service and Operations organization, which is staffed by full-time Securus employees.

Services and Operations Organization

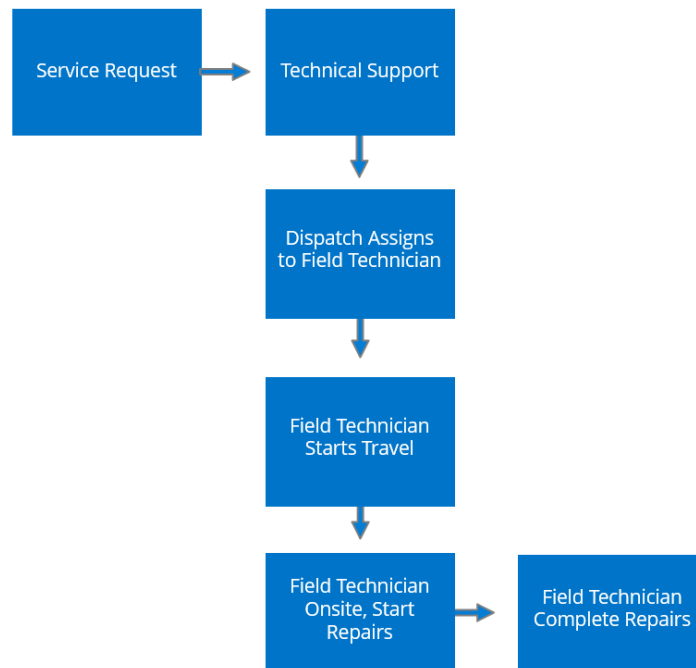


Securus adopted this operational model because of the natural interaction between functional groups. Having our support services integrated and centrally managed enables cross-functional group interaction, improving the response time, and efficiencies of our services.

Call Routing

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.

Trouble Ticketing Process



In all instances, service will be requested through the TSC and field service personnel will be dispatched through trouble ticketing system to ensure documentation and timely resolution of all service tickets.

Event Tracking System

The Securus event tracking system logs, tracks, manages, and assures an appropriate response to all service requests. The service request generates a unique trouble ticket number linked to each facility's service history and provides real-time updates. Each ticket has a priority level assignment, which drives diagnosis and response processes. The support technician performs initial problem diagnosis and isolation procedures, determines the nature of the problem, and resolves the problem or engages the appropriate party for problem resolution.

The TSC maintains ownership of all service requests and responsibility for the escalation and update functions. Every effort is made to resolve problems remotely and within the framework of resolution timeframes. However, if the problem requires on-site service, a

technician is dispatched. Securus will contact the facility to arrange for the on-site service at the convenience of the facility.

Facilities can also use Securus' request portal to create self-help tickets and monitor and track ticket status.

Facility Service Request Portal



WA DOC can access Securus' service request portal as an alternative to calling Securus Technical Support to create new service requests or to track the status of existing service requests.

Securus' service request portal is an automated ticketing system that logs, tracks, manages, and assures appropriate responses to all service requests for a correctional facility, regardless of whether the request was initiated from a call to Securus Technical Support or entered directly into the service request portal.

The service request portal is one of the major tools in our arsenal to meet service level agreements with confidence, increase overall operational effectiveness, solve problems, streamline repetitive tasks, and improve customer satisfaction.

When a facility requires a service visit for any reason, including routine maintenance, a service ticket is opened and visible within the service request portal to track the event and allow for further analysis of any system issues and/or performance.

As with all service requests, those entered directly into the service request portal include information collected on the issue as gathered by the certified technician(s) to ensure our response is appropriate for the service event. Diagnosis of the event will determine whether the request or repair can be performed remotely or if onsite trouble-shooting assistance with our local field technician, working in conjunction with our Network Operations Center (NOC), is necessary. All service events, whether resolved remotely or via an onsite visit, are tracked and our customers can provide feedback on how we have performed and if we met their expectations. Further, the service event will be assessed to avoid repetitive service issues, which may indicate a system deficiency issue or fraudulent activity.

The service request ticketing system is used in various departments throughout Securus to provide a current view of any open items. The system automatically generates reports internally that are sent to management for service level reviews and customer status.

Through the Securus service request portal, WA DOC staff can view, track, and open service tickets; the portal also offers WA DOC the advantage of knowing the status of a resolution or viewing comments on any service request, which results in efficient and effective communication through this direct line of communication without needing to place a call.

Opening a New Service Ticket

SECURUS Technologies

Securus

Create Ticket Search Ticket Administration

Job Id: New Job

Problem Category: **Select Problem Category** (dropdown menu open)

- Select Problem Category
- Full Outage
- Inmate Can't Place Call
- Other
- Partial Outage
- Password Reset
- Phone/Equipment Replacement
- PIN Reset
- SCP User Interface Question

Problem Description: [Text Area]

Create Ticket Cancel

Ticket Number with Detail

SECURUS Technologies

Securus

Create Ticket Search Ticket Administration

Site: [Dropdown] Status: Open [Dropdown]

From Date: 01/01/2018 To Date: 03/21/2019 View Report

1 of 1 Find | Next

Ticket	15830284
Site ID	06388
Site Name	[Redacted]
Address	[Redacted]
Contact	[Redacted]
Product	[Redacted]
Priority	2
Problem Description	Anjanaa testing new job display in portal
Status	New
Solution	[Redacted]
Date Opened	2018-10-29 11:20:52
Last Actioned Date	2018-10-29 11:20:52
Date Closed	[Redacted]

New

Created Date	Created By	Note
[Redacted]	[Redacted]	[Redacted]

In addition to the above processes, the Securus Account Manager assigned to the Washington DOC will be responsible for conducting quarterly business meetings to review the last quarter’s performance against metrics, introduce new product and services and discuss issues. In each meeting, the Account Manager will present reports that identify Securus’s service response times as compared to the agreed to Service Level Agreements. Trends will be reported and required actions will be tracked and presented at the next meeting.

26. Describe your escalation process for resolving phone issues for both DOC and end users.

Vendor’s response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

If resolution is delayed, escalation procedures within Securus Team are activated to ensure appropriate resources are allocated to resolve the problem. For example, when a service ticket reaches the halfway point of the allotted priority-level resolution timeframe, the Technical Support Manager and Field Service Manager (escalation contacts) receive an automatic e-mail. For example, if a P1 priority level has a two-hour response time, an automated e-mail will be sent at one hour, providing the escalation contact with notification of the pending service deadline.

If the ticket exceeds the priority-level resolution timeframe, an automated e-mail is sent to the Technical Support Director will follow the escalation chain below:

Technical Support (All Levels)	
Acuity Level	Contact
Level 1	Technical Support Department
Level 2	Technical Support Manager/Field Service Manager
Level 3	Technical Support Director
Level 4	Regional Field Manager
Level 5	VP Service and Technical Operations

The process described above is the internal escalation process that will be activated automatically through our ticketing process. The DOC will be provided the contact

information for the contact person at the various acuity levels of the escalation chain to be able to follow the escalation process themselves.

Securus Friends and Family Call Center

Securus strives to deliver superior customer service and resolve customer issues in one call. Securus Friends and Family Call Center (SFFCC) supervisors are always available to assist customers when an issue requires escalation. Some issues may require time to research and resolve. For all issues, the following escalation list may be utilized after 24 hours:

- Escalate to customer service manager;
- If still unresolved, escalate to the director of customer care;
- If still unresolved, escalate to vice president of customer care.

27. Describe in detail the circumstances in which you will compensate DOC and refund users, including friends and family, for problems with the phone system.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

To obtain an account refund, end users may contact Securus Friends and Family Call Center (SFFCC) by phone at 800-844-6591, or by chat at www.securustech.net. For all credit card transactions made by phone or website, full and partial refunds will be applied to the payment source last used. For full refunds on accounts last funded via Western Union, funds will be refunded to the customer through Western Union. For partial refunds on accounts funded via Western Union and for both full and partial refunds on payments mailed to Securus, a check will be mailed via the U.S. Postal Service.

Friends and Family AdvanceConnect Accounts

Refunds of unused balances, when provided, are credited back to the credit or debit card used to fund the AdvanceConnect account. If the AdvanceConnect account holder used a prepaid Visa or MasterCard to fund their account, the account holder must maintain possession of the card to ensure they receive their refund. If the AdvanceConnect account holder funded the account through check, money order, Western Union or MoneyGram, a refund check will be mailed to the AdvanceConnect account holder, which could take up to four weeks for processing. AdvanceConnect account holders have 180 days from the date of the last call received on the AdvanceConnect account to request a refund of any unused balance. The balance of the refund may vary based on when calls were last received.

Direct Bill Accounts

Occasionally a Direct Bill account holder may over-pay the bill and request a refund of the amount overpaid. To request a refund, the Direct Bill account holder must call Securus at 1-800-844-6591. There is no charge to the customer to receive a refund in these cases.

Video Visit

Securus video visits are pre-paid and in general are non-refundable. If a user believes there was a system problem that did not allow them to participate in a scheduled video visit, they would have the opportunity to fill out and submit a Video Visitation Refund form.

Consumers can manually request a refund of a credit balance on their Video Visitation account by submitting a Video Visitation Refund form. The form can be obtained by calling Securus Correctional Billing Services.

Refunds will not be granted unless there was a previously approved credit applied to the Securus Video Visitation account. There are currently no refund fees or minimum refund amounts, however, transaction fees are not eligible for refund. Refunds are issued back to the original credit/debit card for which the transaction(s) was paid for.

Securus is not responsible for disconnects due to behavior issues, disconnects initiated by the correctional facility, or disconnects due to internet connection or hardware malfunctions. If the user believes their session was disconnected due to a Securus Video Visitation system error, they should fill out and submit a Credit Request Form. Securus will review and reply to the request within 72 hours.

Once scheduled, a Video Visitation session must be attended during the scheduled time period. Failure to sign on at the scheduled time or signing on late will not extend the session time period for which the user paid.

In limited situations, Securus may, at its discretion, offer a credit for a scheduled and paid Video Visitation session. A credit is defined as funds used to pay for a session being placed back on to the user's account, which are available for use for another future Video Visitation session. Credits may occur when a) the facility cancels a paid Video Visitation session before the session begins, b) the facility rejects a paid Video Visitation session prior to it starting, and c) Securus cancels a paid Video Visitation session before the session begins. Credits will not be given for sessions where the scheduled time has started or prior to session completion. Credits shall expire 90 days from date of issue.

28. Service calls and Vendor's responses must be documented and maintained and DOC must receive a monthly report detailing the service issues. Describe how you will meet this requirement.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus maintains records on all service calls and will provide WA DOC a monthly report. WA DOC staff can also review the status of an individual ticket through the Facility Service Request portal.

In addition to the above processes, the Securus Account Manager assigned to the Washington DOC will be responsible for conducting quarterly business meetings to review

the last quarter's performance against metrics and discuss issues. In each meeting, the Account Manager will present reports that identify Securus's service response times as compared to the agreed to Service Level Agreements. Trends will be reported and required actions will be tracked and presented at the next meeting.

Facility Service Request Portal



Securus' Facility Service Request portal documents and maintains records of every ticket generated by a service request. WA DOC personnel can access the service request portal track the status of existing service requests and review records of completed requests.

Securus' service request portal is an automated ticketing system that logs, tracks, manages, and assures appropriate responses to all service requests for a correctional facility, regardless of whether the request was initiated from a call to Securus Technical Support or entered directly into the service request portal.

The service request portal is one of the major tools in our arsenal to meet service level agreements with confidence, increase overall operational effectiveness, solve problems, streamline repetitive tasks, and improve customer satisfaction.

When a facility requires a service visit for any reason, including routine maintenance, a service ticket is opened and visible within the service request portal to track the event and allow for further analysis of any system issues and/or performance.

As with all service requests, those entered directly into the service request portal include information collected on the issue as gathered by the certified technician(s) to ensure our response is appropriate for the service event. Diagnosis of the event will determine whether the request or repair can be performed remotely or if onsite trouble-shooting assistance with our local field technician, working in conjunction with our Network Operations Center (NOC), is necessary. All service events, whether resolved remotely or via an onsite visit, are tracked and our customers can provide feedback on how we have performed and if we met their expectations. Further, the service event will be assessed to avoid repetitive service issues, which may indicate a system deficiency issue or fraudulent activity.

The service request ticketing system is used in various departments throughout Securus to provide a current view of any open items. The system automatically generates reports internally that are sent to management for service level reviews and customer status.

- 29. Describe, in detail, your service level for phone maintenance including maintenance schedule. Maintenance should be performed at all facilities, including work releases, on a regular schedule.**

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

It is Securus standard operating procedure (SOP), that our Field Service Technicians perform Preventative Maintenance (PM) at every site every site at least once a month. Upon awarding of the contract Securus will work with WA DOC personnel to create a customized Preventative Maintenance schedule. Preventative Maintenance includes:

- Inspecting and testing of individual phones/terminals and associated hardware
- Cleaning out the system filters
- Testing system features and functionality
- Performing workstation(s) inspections.

Additionally, our FSTs also perform preventative maintenance whenever they are dispatched to the site for any reason. Upon resolving the primary issue, the Field Service Technician will perform a system check to detect any unreported issues. Problems identified during this check are addressed by the FST during the same visit unless additional parts are required to resolve the issue.

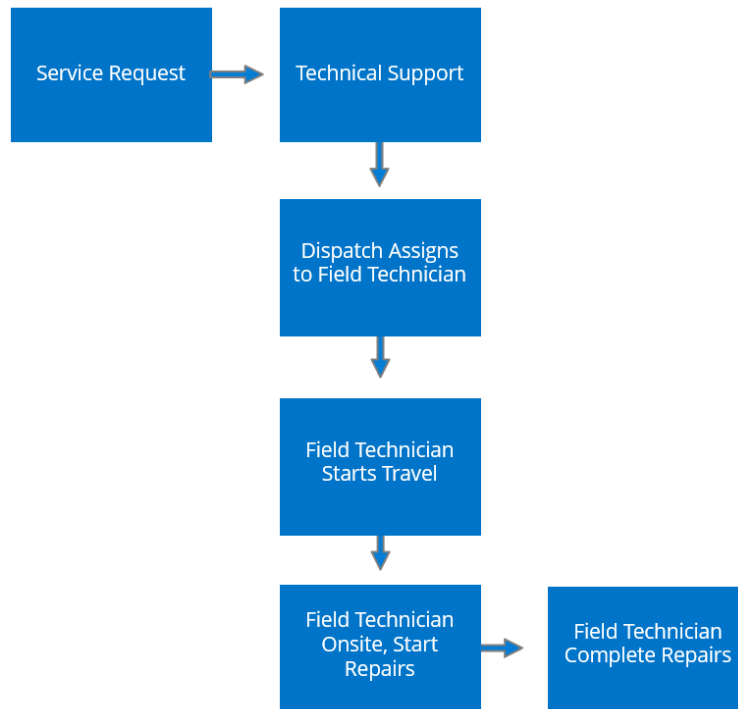
Service Levels

The technical support team at our Technical Support Center (TSC) has primary responsibility for resolution when a problem occurs or when maintenance is needed outside the set schedule. If the issue requires on-site service, the dispatch team at the TSC contacts the assigned field service technician (FST) and establishes an estimated time of arrival. The Dispatcher or the FST immediately communicate the time of arrival to the facility. Upon arrival at the facility, the FST will meet with the primary site contact to review the problem and perform the necessary repairs. Repairs typically involve repairing or replacing a defective part or wiring, or correcting configuration settings.

After completing the repairs, the FST confirms the resolution with the primary site contact and obtains sign-off on the repairs performed. After obtaining sign-off, the FST will record the transaction in our service ticket management system through his or her laptop.

The TSC manages the flow of inbound calls through a call distribution system that routes calls directly to our support technicians in a skills-based, platform specific manner. Securus establishes response times and service level agreements that accomplish our key objective of providing timely resolution to each request. Service calls are answered 24x7x365 by live technicians to provide timely and quality customer service.

Trouble Ticketing Process



When a facility contacts Securus, an event tracking system assigns a trouble ticket, with one of three initial priority levels—P1, P2, or P3. Each level is designed to address specific system events and has a prescribed resolution timeline and escalation procedure. In all cases, Technical Support will respond to the customer within the required timeframe.

Priority 1 Service Level

A Priority 1 (P1) assignment—our highest priority assignment—occurs when a system event adversely affects 30 percent or more of system functionality. Examples of P1 service assignments include:

- Voice prompts not operating
- Features are not operating appropriately
- CD-burning abilities disabled
- Live call monitoring is not operating appropriately
- NextGen SCP access denied
- All phones out-of-service

The response time for a P1 event is two hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

A P1 events escalate to:

- Technical Support Department
- Technical Support Manager
- Technical Support Director
- Regional Field Manager
- Executive Director of Service

If the problem resolution is delayed, escalation procedures within the Securus Management Team are activated to ensure appropriate resources are allocated to resolve the problem.

Priority 2 Service Level

A Priority 2 (P2) assignment—our mid-level priority assignment—occurs when a system event adversely affects 5 to 29 percent of system functionality. Examples of a P2 service assignment include problems or errors with related to:

- Workstation
- Specific system ports
- Local Exchange Carrier (LEC) circuits
- Unblocks
- Blocked numbers
- Missing call detail records (CDRs)
- Call searching

The response time for a P2 event is 24 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P2 events escalate to the Technical Support Department.

Priority 3 Service Level

A Priority 3 (P3) assignment—our lowest priority assignment—occurs when a system event adversely affects 5 percent or less of system functionality. System events adversely affecting some of available facility phones. Examples of P3 service assignments include:

- Static on the phone
- A party's inability to hear
- An incarcerant's inability to dial
- A broken phone
- Non-functioning dial pad
- Non-functioning cutoff switches

- An inability to generate reports

The response time for a P3 event is 72 hours. If a dispatch is not required, Securus notifies the facility upon issue resolution. If a dispatch is required, Securus contacts the facility and provides an estimated time of arrival.

P3 events escalate to the Technical Support Department.

30. Describe the phone network operation monitoring capabilities available to DOC.

Vendor's response:

SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus continuously monitors all data centers, infrastructure components, platform systems, and communications services using the SolarWinds® suite of network performance monitors. The SolarWinds® 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 Secure Communications Platforms™ (NextGenSCP™), 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.

SolarWinds® Typical Monitored Application Elements

Average CPU Load & Memory Utilization

THRESHOLDS EDIT HELP

Avg CPU Load: 9%
Memory Used: 57%

Average Response Time & Packet Loss

THRESHOLDS EDIT HELP

Avg Resp Time: 0 ms
Packet Loss: 0%

Monitored Sessions

EDIT HELP

Total Calls: 22

Current Sessions - Monitored Sessions
MIN/MAX Average Statistic Data
TODAY (Every Hour)

Top CPUs by Percent Load

EXPORT EDIT HELP

Mar 24 2019, 1:40 pm - Mar 25 2019, 1:30 pm

Network Latency & Packet Loss

EXPORT EDIT HELP

Mar 25 2019, 12:00 am - Mar 25 2019, 1:30 pm

Legend: Response Time, % Packet Loss

Disk Volumes

EDIT HELP

VOLUME	SIZE	SPACE USED	PERCENTAGE
C:\ Label: 34609856	278.3 GB	55.2 GB	20%
D:\ Label: Data 2c7978c4	557.6 GB	164.6 MB	0%
Physical Memory	31.9 GB	18.2 GB	57%
Virtual Memory	36.7 GB	19.6 GB	53%

Components

EDIT HELP

COMPONENT NAME	STATISTIC	MESSAGE	RESPONSE TIME	PORT
ActiveCallsCurrent	440		0 ms	N/A
ActiveCallsMax	465		0 ms	N/A
CallDenialsCurrent	0		0 ms	N/A
CallsTotal	749		0 ms	N/A

Last Events

LAST 3 MONTHS

3/6/2019 2:36 PM [icon] rebooted at 3/6/2019 3:36:00 PM

Hardware Details

EDIT HELP

Server

Hardware Status: Up
Manufacturer: Dell Inc.
Model: PowerEdge R630
Service Tag: [redacted]
Last Poll Time: 3/25/2019 1:34:49 PM
Dell OpenManage: v9.1.0

Current Hardware Health

MANAGE SENSORS EDIT HELP

SENSOR NAME	STATUS	VALUE
Fan	OK	
Power Supply	OK	
Temperature	OK	
Disk	OK	

Disk Volumes

EDIT HELP

VOLUME	SIZE	SPACE USED	PERCENTAGE
C:\ Label: 34609856	278.3 GB	55.2 GB	20%
D:\ Label: Data 2c7978c4	557.6 GB	164.6 MB	0%
Physical Memory	31.9 GB	18.2 GB	57%
Virtual Memory	36.7 GB	19.6 GB	53%

Current Percent Utilization of Each Interface

EDIT HELP

STATUS	INTERFACE	TRANSMIT	RECEIVE
Up	Intel(R) Gigabit 4P I3504 nDCC - LAN1	0%	0%
Up	Intel(R) Gigabit 4P I3504 nDCC #3 - LAN3	0%	4%
Up	Microsoft Network Adapter Multiplexor Driver - Team1	0%	2%

Application Overview

Application Count: 51

51 Up, 0 Warning, 0 Critical, 0 Down, 0 Unknown, 0 Other

Securus Network Operations Center in Dallas, TX



Premium Network Monitoring Capabilities

Securus proactively identifies potential system and network abnormalities through SolarWinds® suite of network performance monitors. This software allows Securus personnel to monitor all hardware, software and system metrics continuously.

Through network monitoring Securus can:

- **Proactively repair systems to prevent outages.** Many times corrections are made before a facility is aware of a problem. This means less downtime and increased system reliability for the facility.
- **Alert remote or on-site engineers of system threshold inconsistencies or alarms.** The NOC communicates with engineers through e-mail, short message service (SMS), or directly through a wireless phone to address the issue.
- **Receive real-time alerts when the system detects an error.** Monitoring identifies if network elements exceeded established thresholds and alerts Securus personnel of possible carrier network issues.

- **Ensure sufficient resources are in place.** The Securus capacity engineering team reviews call traffic volume reports and storage requirements throughout all systems to ensure sufficient network capacity.
- **Centrally monitor calling traffic to determine increases or decreases in the number of telephones.** With DOC agreement, the service and operations team will install additional telephones when required.

Remote Programming, Diagnostics, and Troubleshooting

The Securus NOC monitors the NextGen SCP platform and our network. The NOC can contact the Technical Support Center (TSC) if it determines that another level of technical support is needed to address an issue. This action could involve dispatching a Field Service Technician to a WA DOC facility.

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.

SolarWinds® Facility Monitoring Example



In addition to real-time monitoring and alerting, Securus Technical Support also leverages the SolarWinds® 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. Additionally, change control practices have been reviewed and are compliant with Sarbanes-Oxley.