Video Visitation Requirements.

Respond to each of the items below.

1. **Equipment to facilitate video visitation (i.e. kiosks or other methods of facilitating the visits) must be installed in each dayroom of each Department facility including IMU North at WSP (other IMUs are excluded). Acknowledge your acceptance of this requirement.**

   Vendor’s response:

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

   Securus acknowledges and accepts this requirement.

   Securus currently uses the sPhone XL for video visitation. Coming soon is the XL2, which will be the latest terminal for video visitation.

   **sPhone XL**

   The Securus Video Visitation terminal is a correctional-facility grade, tamper-proof steel enclosure. The hardware is wall mounted unit equipped with a built-in shatter resistant touch screen, a high-resolution video camera with integrated lighting, and tamper-proof, heavy molded plastic handset with an armor-reinforced cord for audio communication, and surge protection.

   The proposed sPhoneXL terminals include, at a minimum, the following:

   - A detention grade hardened steel enclosure
   - One detention grade audio handset per terminal for the incarcerant, and two detention grade audio handsets per terminal for the public
   - A shatter resistant LCD monitor with integrated camera
   - Enclosures which prevent spills from entering
   - Terminals that do not have any openings exposed to the user, including all wiring and ventilation holes
   - Terminals without any external hinges
   - Terminals are powered by 110 VAC, low voltage DC, or IEEE802.3at (PoE Plus).
   - Rounded tops and corners
   - Terminals with built-in LED lighting that automatically activates during video visitation sessions and automatically ends when the video visitation session completes and/or disables during all other functions
   - Terminals that use standards based videoconferencing CODEC
   - Terminals with multiple mounting methods: wall, table, pedestal or cart. All mounting options use standard industry or better methods
   - Options for powering the units on and off
Technical Specifications

- Light and ruggedized vandal-proof terminals (hardened steel): Best balance between weight and resistance
- Sealed: Dust and Liquids Resistant, spill-proof (accidental or deliberate).
- Assembly elements are hidden: No screws or hinges can be removed and used to manufacture weapons. No doors/compartments that can be opened in the front or on the sides of the unit.

- Rounded edges that reduce the risks of accidental or intentional injuries.
- Abrasion and chemical resistant; the unit can be cleaned using commercial cleaning agents.
- Humidity and corrosion resistant
- Built-in LCD 15” with hardened shatter resistant touch screen
- HD camera, autofocus, (720p @ 30 fps)
- Sphone XL PoE has movable camera with a 2MP (1600x1200) resolution
- Optional hands free terminal with built-in HD video camera, Pan-Tilt-Zoom, 10x optical zoom, 4x digital zoom, 30fps
- Built-in LED lighting system & Power ON LED indicator
- Magnetically activated pushbutton for on/off power
- Built-in heat sink mounted to the back for heat dissipation
- Built-in protection device against voltage variations
- Vandal-proof handset. Armored cable
- Standard non-proprietary computer components
- All electrical components comply with UL, CE and/ or CSA
- System maintenance via wireless keyboard (Infra Red Access)
- Mother board: Micro/Mini ATX
- Intel Quad Core 2 GHz processor
- Memory: DDR3; RAM 4,096 MB (4 GB)
- Solid State (SSD) Hard drives to reducing moving components and potential failure points.
- Network: Ethernet RJ-45 (CAT5/6)
- Power Options:
  - AC: 110V 2 amps
  - Low voltage DC: 24 V 8.33 amps
  - Power over Ethernet: IEEE802.3at (PoE Plus).
XL2

At the core of incarcerant services is the new XL² Incarcerant Kiosk. Incarcerants use this kiosk to access digital content (music, movies, games, educational materials, and news), compose (or upload) and send email, send eCards, attend video visitation sessions, log into their JPay account, and send grievances to facility staff. It can also support any Securus-based services available via the current sPhone XL terminal and its ConnectUs application suite, which means that a single kiosk installation can handle all of the DOC’s offender communications needs.

The kiosk incorporates a standard size keyboard, trackball mouse, and wrist rest space. It accommodates numerous mounting options, such as wall, tabletop, cart, and pedestal.

Kiosk Specifications

- Hardened steel enclosure with anti-vandal security lock and bolts
- Built-in LED Lighting
- Dimensions: 22¾ “x 21” x 4¼ ”
- Weight: 50 lbs. (including PC & networking components)
- High strength scratch-resistant security glass
- Dynamic handset with secured caps and a 32” armored cord
- Stainless steel keyboard with trackball and braille keys
- Power - Power over Ethernet, 802.3at (PoE+), 25 watts
- MTBF: 80,000 hours
**Encased Components**

- 17” LCD hardened touchscreen monitor with integrated privacy screen
- Screen resolution 1280x1024
- 5 megapixel autofocus camera with 2592x1944 max resolution
- Quad core processor
- 4 GB RAM
- 512 GB mSATA hard drive
- Armored USB cable
- Cat6 Ethernet Port

The keyboard and trackball are resistant to liquid, dust, and debris. The keyboard is integrated into a sealed metal base so that its components are spill-proof. The kiosk is also designed so that spilled liquids flow away from important componentry if they do somehow reach the inside of the kiosk. All electrical components are compliant with UL, CE, and/or CSA standards.

Parts can only be removed from a kiosk by a technician. Kiosks are vandal-proof and are treated well because they provide a valuable service to the incarcerant population.

Kiosks have smooth stainless steel surfaces with no sharp edges. If cleaning is necessary, kiosks are easily wiped down since all exterior parts are water-resistant, including the keyboard and handset.

Technicians can quickly open the enclosure and swap components. Components are designed and fastened so that the technician can quickly detect a problem and replace a particular component, most of them, or all of them if necessary.

2. **Incarcerant friends and families must be able to connect to incarcerants using widely available equipment including webcams connected to personal computers and via cameras on portable devices and cell phones. Describe how Vendor will meet this requirement.**

Vendor's response:

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

Securus offers anywhere video visitation, which allows remote visitors, such as family and friends, bail bondsmen, probation officers, and attorneys secure communication with incarcerants from outside the facility via a broadband internet connection on any device, including both Android and Apple mobile devices.

Remote visitors access Securus Video Visitation (SVV) services through the Securus mobile application or the Securus Online website, at www.securustech.net. Remote users need only a tablet, computer, or mobile phone with a built-in or external webcam and a microphone and speakers, or a headset.
Family and friends can obtain an approved account profile remotely by sending their picture and driver’s license. *Securus is the only company that offers this feature.*

From the mobile app or website, visitors select the facility and incarcerant with whom they would like to visit and then can:

- Create, reschedule, and/or cancel a scheduled video visit session
- Pay for the scheduled session with a credit or debit card
- Apply for remote video visitation privileges from the facility
- Join a visitation session with incarcerants—no officer intervention is required

3. **System must provide a function for visitors and incarcerants to perform a round-trip test of their equipment/personal device (webcam, phone, etc.) to see if it can adequately handle video visits through the System. Describe how Vendor will meet this requirement.**

Vendor’s response:

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

Visitors must register for a Securus Video Visitation account at [www.securustech.net](http://www.securustech.net) or through the mobile application to be able to conduct video visitations. As part of the registration process, the Securus Video Visitation (SVV) system will verify that the visitor’s computer system is compatible with SVV. The system check includes verification that the webcam works properly.
Incarcerant Video Visitation Terminal

The XL terminal is made to perform video visitations and Securus will maintain them in working order to make sure they can be used to perform video visitations through the system.

4. Visits must occur in thirty (30) minute blocks, with the ability to extend for an additional thirty (30) minutes as facility resources allow. Describe how Vendor will meet this requirement.

Vendor’s response:

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

The Securus visitation system will be configured to set visitations in thirty (30) minute blocks. When scheduling a visit, the system will prompt the visitor with only the approved and available minute blocks when choosing the duration of the visit.
5. The System must have the ability to allow visitors to request a visitation time slot using the Vendor’s public portal and require incarcerants to confirm availability (please note that different facilities may have different schedules). Describe how Vendor will meet this requirement.

Vendor’s response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The SVV scheduling software will only display the available time slots based on incarcerant availability, restriction status, and incarcerant’s cell block locations. When a user logs on to the video visitation website or mobile app, they select the facility and incarcerant they wish to visit. The system shows the available dates and times from which they can pick; through an integration with the incarcerant management system, the application automatically schedules visits according to the incarcerant’s housing location, available terminals at that location, and available visitation time slots.

Scheduling Features for Family and Friends Members

Securus Video Visitation (SVV) makes the complex tasks of scheduling sessions and managing user accounts easy and secure for the family, friends member or other visitor. The list below provide some of the associated features and functions – inherent in SVV – required for successful deployment.

Visitors may access their SVV account and schedule visitation sessions for approval any web-enabled device by going to www.securustech.net of or from the Securus mobile app. Visitors can also reschedule or cancel their visitations through their SVV account.

- Web-based and accessible from any standard web browser or from the SVV mobile app, available for both Android and Apple
- Simple user interface, enabling account setup and scheduling to be completed in minutes
- Automatically support multiple facilities in multiple locations with multiple housing units, making it easy to “find” the desired incarcerant
- Automatically display only the visitation times and dates that are available
- Automatically send an email confirmation when a visit is scheduled, modified, or cancelled
- Allow users to easily change their personal information (password, address, phone number, etc.)
Secure, At-Home Visitation Scheduling

Step-by-Step Scheduling Process

1. User goes to “My Account” and selects “Schedule a Visit” under the video visitation section.
2. Select the type (remote or onsite) of visit at the site of the incarcerant with whom the user wants to visit.

3. Enter the incarcerant’s information to search for the correct incarcerant.
4. Select the correct incarcerant and click “Next.”

**Search For Inmate**

Search by  
- Inmate Name
- Inmate ID

First Name  Last Name
Sara       Sullivan

**SEARCH RESULTS**

<table>
<thead>
<tr>
<th>INMATE</th>
<th>INMATE ID</th>
<th>STATE</th>
<th>FACILITY</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sara Sullivan</td>
<td>#60017798683</td>
<td>TX</td>
<td></td>
</tr>
</tbody>
</table>

**Appointments Summary**

- **Visitaton Type:** Remote
- **Site:** TX
- **Inmate:** Sara Sullivan
- **Duration:**
- **Date:**
- **Time:**

Select Inmate

If the inmate you were looking for is not listed, please verify the inmate information and try again.
5. Select the relationship to the incarcerant, the duration of the visitation session, and the date and time of the visit. Note: The visitor must agree to the terms and conditions before submitting the request.

- Schedule (1) Visit
  - Schedule and pay for (1) visit

**Relationship To Inmate**

- Relationship

**Appointment Details**

- Duration
- Date
- Time

I have read and agree to the Terms and Conditions.
6. Washington State Department of Children Youth Family Services (DCYF) Social Workers and contract providers are frequently court ordered to facilitate video visits between minors and their incarcerated parents. The proposed video visitation System must provide a mechanism for billing DCYF directly for the cost of the video visit for these supervised minors. Note that state law prohibits state agencies from paying for these services in advance and this includes establishing a credit card on file with a vendor. Describe how Vendor will meet this requirement.

Vendor’s response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will work directly with DCYF to customize an arrangement that facilitates the ability of court-ordered video visitation visits between minors and incarcerated parents to be paid by DCYF, and done so after the visits have occurred and consistent with state law (such as not billing the visits to a credit card).

Video visitation in NG SCP can readily provide a monthly report of completed SVV visits related to DCYF. Based on the pricing to DCYF, the cost for each visit can be calculated. Based on the calculated costs and an invoice can be prepared and sent to DCYF.
7. The System must provide the ability for the Department to limit the users of the System to only those approved by the Department. 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™) will provide the Department the ability to limit facility, friends and family, and incarcerant users to meet their security goals.

Limiting Facility Users

NextGen SCP™ provides an advanced, multi-level password scheme specifically designed to provide facility administrators the ability to use unique security roles to determine user permissions. Security roles define what actions a user can and cannot do within the system. NextGen SCP contains default security roles, identified by the eyeball (👀) icon. While these predefined roles cannot be modified, they cover many customers’ needs for granting access and denial rights based on common job functions.

NextGen SCP provides more options for WA DOC to further customize access privileges by allowing authorized administrative users to either create a new user-defined role or create a new role using an existing role as a base and further modifying it. The user-defined role can be customized to meet the DOC’s specific needs when a default role does not. These roles are identified by the pencil (✍️) icon.

In addition, the WA DOC administrator can assign multiple roles to a user to tailor their access to exactly what is needed. This provides virtually unlimited options for customizing users’ access. Please find sample security rolls on the following page.
Sample Security Roles

Limiting Friends and Family Users

Securus' video visitation system allows WA DOC to authenticate and approve a visitor user through the online account registration process. Visitors can easily register from any web-enabled device by going to www.securustech.net. When the facility staff approves the account request, the visitor receives an email notification that they have been approved and can now schedule their visit.

Attorneys have a separate registration process from the general public. Attorney accounts will require additional verification, such as a Bar ID.

After completing the process, facility personnel must approve and authorize the user's registration before visitation sessions can be scheduled. This process allows the DOC to verify a visitor's eligibility to visit with an incarcerant. NextGen SCP brings a new option to visitor approval. WA DOC can choose to manually approve all visitors or have the system automatically approve visitors. If automatic approval is the default, WA DOC staff can always review the contact profile and manage the visitor as needed.
Securus Online Registration Process for the Visitor

Step 1: Email & Password

Users will need to complete provide an email and password. Fields with a red asterisk are required.

Step 2: Security Questions

Users must select three security questions and provide corresponding answers to help protect the user’s account security.
Step 3: Security Questions

Users must provide current contact information to complete the account set up.
Step 4: Sign up for Video Visitation

Users need to sign up for video visitation and will need to select a user type—friend/family member or attorney.

Step 5: Photo

Users will verify their computer system is compatible with SVV. This system check includes verification that the web camera works properly.
Step 6: Document Upload

Users are required to submit a profile photo and a photo of their government ID for the facility to approve them as visitors.

Document Upload

SIGN UP FOR VIDEO VISITATION

1  2  3  4
User Type  System Check  Document Upload  Facility Selection

Video Visitation

You must take two photos to submit for approval to the Correctional Facility. Click the camera image below to take your photos using your computer’s web camera.

In order to add Securus Video Visitation to your account, you are required to take a photo of your government issued photo ID and a photo of yourself. These images will be added to your Securus Online account and will be submitted to the correctional facility for approval where you would like to visit with an inmate.

Profile Photo  Government ID

[Images of profile photo and government ID]

*Users are given 10 minutes to complete each of the four account creation steps before the software automatically times out.

Step 7: Facility Selection

Users must select the facility where their incarcerant is located.

Facility Selection

SIGN UP FOR VIDEO VISITATION

1  2  3  4
User Type  System Check  Document Upload  Facility Selection

Please select the state of the Correctional Facility where the Inmate is housed.
If you are unable to locate the facility, please review Facilities We Serve.

State
Select

[Submit button]
After completing the process, facility personnel must approve and authorize the user’s registration before visitation sessions can be scheduled. This process allows the WA DOC to verify a visitor’s eligibility to visit with an incarcerant. NextGen SCP brings a new option to visitor approval. WA DOC can choose to manually approve all visitors or have the system automatically approve visitors. If automatic approval is the default, WA DOC staff can always review the contact profile and manage the visitor as needed.

Sample Window of Pending Visitors

Manual Approval of Appointment

Additionally, WA DOC will have another opportunity to limit users of the system through the manual approval of visitations, if the Department chooses to implement this configuration. WA DOC can be configured for manual approval of all scheduled visitations. This configuration would provide the DOC the opportunity to authenticate that the scheduled visit is taking place the applicable approved or scheduled visitor.

Authorized facility staff will have the ability to review and approve appointments in SVV through the NextGen SCP user interface. In the SVV widget the user will find a list of...
appointment needing approval. The user would approve the visit by clicking on the green check mark icon or reject the visitation by clicking on the red X icon.

Each requested appointment includes the session ID, type of user, name of incarcerant, housing location for incarcerant, terminal where the visitation is assigned, visitor name and a link to the visitor's pictures.

Limiting Incarcerant Users

Authorized WA DOC users can suspend an incarcerant for a predetermined amount of time through the NextGen SCP user interface. Suspension can occur across all communication system applications, except for attorney’s visits.

To suspend an incarcerant, the user simply logs in and goes to the “manage” tab and selects incarcerant. They will be provided a page where they can search for the incarcerant they want to suspend by using the omnibox search field at the top.

Users can search by incarcerant name, account number or PIN. Once on the incarcerant's profile page, the user can suspend the incarcerant by clicking on the pencil icon, for the desired application.
A window with then pop-up where the user can select the timeframe for the suspension.
8. All visits must be recorded, and must be able to be monitored in real time and ended remotely by Department staff as the visit is occurring. Describe how Vendor will meet this requirement.

Vendor’s response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

With Securus’ NextGen SCP, recorded visits are searchable and viewable in live or archived sessions. Authorized WA DOC users can search and view video visitation from the “monitor” tab on the user interface. They will have the choice between viewing a single session for multi-session.

If the user chooses to view a single session, they can filter their search for the desired visitation session by site, terminal group and phone. From the results page, the WA DOC user can launch monitoring and view the visitation by clicking on icon.
Multi-Session Monitoring Window

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

How it Works

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

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

- Visit type
- Visitor type
- Incarcerant terminal group or individual terminal
- Visitor terminal group or individual terminal
Sessions are displayed in the order in which they began, beginning in the upper left corner. For example, if a WA DOC facility has 12 sessions all scheduled to begin at 1:00 p.m., the first session in the upper left of the MSM window will be the visit where both the visitor and incarcerant joined first.

**Multi-Session Live Monitoring Zoom-In Window**

Authorized WA DOC users can zoom in on an individual video visitation session, allowing for even more capabilities, such as listening to the audio or immediately disconnecting a visit. After zooming in, a user can stop monitoring that specific session or cancel the visitation session by selecting the icon in the lower right of the screen, if inappropriate behavior is seen.
Securus Video Visitation Barge In

A new feature of our video visitation is SVV Barge In, which allows WA DOC staff to break in to an ongoing video visitation session to send a pre-defined visual message. This message can be delivered to the incarcerant, the visitor, or both parties simultaneously, in English or a second language. This feature is available in both single session and multi-session monitoring.

To provide WA DOC additional control and options, Barge In can be configured at the site level, and each site can have a unique list of messages from which staff can choose.

SVV Barge-In Messages, Facility View

SVV Barge In Messages, Incarcerant View
Ending a Video Visitation

Authorized users can manually terminate a video visitation session by from either the visitations page or from the live monitoring page. The visits page shows the visits schedule for the day. If the visitation session is in progress, the visitation listing will include an icon, which the user can click to terminate the visitation.

From the live monitoring window, WA DOC personnel can terminate the visitation session by clicking on the red X in the bottom right corner of the window.
Supplemental Monitoring through Guarded Exchange (GEX)

To support WA DOC in video visitation monitoring, Securus will provide live monitoring powered by Guarded Exchange (GEX). Guarded Exchange (GEX), is a wholly-owned subsidiary of Securus, whose trained analysts live monitor visitations in real time for policy violation. GEX will terminate visits that violate Agency Video Visitation Protocols. If a visitation is terminated, the reason why is documented and provided to the DOC in a daily report. If GEX notes something on a visit where it is believed that the safety and security of the facility could potentially be compromised, the analyst will alert the agency directly.

9. **Vendor will monitor video visits to ensure users comply with DOC policy requirements and vendor user agreements. Vendor will provide DOC with weekly reports of video visits that appear to be out of compliance with policy and/or user agreements. Describe how Vendor will meet this requirement.**

Vendor's response:

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

Securus provides for live monitoring of all video visitations sessions by authorized WA DOC personnel through the NG SCP user interface. There is the option for multi-session monitoring or zooming in on one specific visitation. While monitoring a video visit if WA DOC personnel see that the participating parties are not complying with DOC policies they can use the video visitation Barge In feature to send a visual warning to the incarcerant and visitor. SVV Barge In allows staff to break in to an ongoing video visitation session to send a pre-defined visual message. This message can be delivered to the incarcerant, the visitor, or both parties simultaneously. This text-based barge-in feature automatically captures the sent message and other pertinent data and includes it as a part of the visitation communication detail record (CDR). An indicator on the CDR denotes that the Barge In feature was used during the video visitation session. Authorized WA DOC users can then use the Barge In feature as a filter when searching CDRs to create the desired report.

Securus records and creates a communication detail record for all video visitations. NG SCP’s™ dedicated report writer can then be used to create investigative information based on the communication detail records on a weekly basis or for whatever timeframe WA DOC desires. Users can search and analyze communication details on all communication events through NextGen SCP. These details include date, time, duration, telephone number, origination, destination, incarcerant ID, termination reason, and more. Users can customize the standard reports by varying search criteria and then exported in:

- Microsoft® Excel
- CSV (Comma Separated Values)
- Adobe® PDF
Video Visitation Monitoring through Guarded Exchange

To support WA DOC in video visitation monitoring, Securus will provide live monitoring powered by Guarded Exchange (GEX). Guarded Exchange (GEX), is a wholly-owned subsidiary of Securus, whose trained analysts live monitor visitations in real time for policy violation. GEX will terminate visits that violate Agency Video Visitation Protocols. If a visitation is terminated, the reason why is documented and provided to the DOC in a daily report. If GEX notes something on a visit where it is believed that the safety and security of the facility could potentially be compromised, the analyst will alert the agency directly.

Sample GEX Video Monitoring Report

<table>
<thead>
<tr>
<th>Appointment ID</th>
<th>Offender First Name</th>
<th>Offender Last Name</th>
<th>Offender Location</th>
<th>Duration</th>
<th>Start Time</th>
<th>Comments</th>
<th>Initials</th>
</tr>
</thead>
<tbody>
<tr>
<td>1639064</td>
<td>Home</td>
<td></td>
<td></td>
<td>0400</td>
<td>10:30 AM</td>
<td>Completed</td>
<td>AM</td>
</tr>
<tr>
<td>1639065</td>
<td>Home</td>
<td></td>
<td></td>
<td>0400</td>
<td>10:30 AM</td>
<td>Completed</td>
<td>AM</td>
</tr>
<tr>
<td>1639066</td>
<td>Home</td>
<td></td>
<td></td>
<td>0400</td>
<td>10:30 AM</td>
<td>Completed</td>
<td>AM</td>
</tr>
<tr>
<td>1639067</td>
<td>Home</td>
<td></td>
<td></td>
<td>0400</td>
<td>10:30 AM</td>
<td>Completed</td>
<td>AM</td>
</tr>
</tbody>
</table>

10. The System must store digital copies of all visits for a period of 1 year and allow authorized staff to review those videos on demand. The System must track when the video had been accessed and by whom. Describe how Vendor will meet this requirement.

Vendor’s response:

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

Securus will store visitation recordings in accordance with industry standards that will allow for immediate access online for one year as required. Video recordings are stored in Securus’ centralized Disaster-Resistant Carrier-Class Data Centers located in Dallas and Atlanta. The Data Centers house commercial-grade, high-performance, managed video visitation systems built to the latest technology standards. These centers manage all of the hardware and software controlling fraud detection, investigative features, visitation processing, visitation records, and actual recordings of visitations. They are managed under the direct supervision and immediate hands-on maintenance by trained data center
personnel. In addition, all equipment used to store recordings is monitored by the Securus' fully staffed Network Operations Center 24 hours a day, 7 days a week, and 365 days a year.

The NextGen Secure Communications Platform™ (NextGen SCP™) provides a unique set of features and advanced technologies to store communication recordings. Traditional premises-based platforms use local hard drives that may fail and are susceptible to local disasters. Premises-based systems need manual backup schemes that are unnecessary with NextGen SCP. NextGen SCP writes all recorded communication events to a Network Attached Storage array (NAS) in our primary data center. Each NAS array is also replicated to the secondary data center for redundancy and failover. All recordings created on the platform reside in at least two of our data centers. Recordings can be downloaded from NextGen SCP in various, widely-used formats and copied to a CD, DVD, or other portable media.

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 can scale by adding another node of dense SATA disk to the storage array. Within the NAS, NextGen 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 communication records and recordings are retained in secure, disaster-resistant locations.

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
Video Visitation Recording Search and Retrieval

Authorized Jefferson Parish users can generate communication reports on all Securus Video Visitation (SVV) events through the NextGen Secure Communications Platform™ (NextGen SCP™) user interface using the process describe earlier on in this response. Jefferson Parish users can perform a dynamic search using the single-input omnibox or an advanced search.

Searching for SVV Events

As with call recording, the search results will indicate whether or not the communication detail record (CDR) has an attached video recording with the presence the icon.
Tracking who has accessed a visitation

NextGen SCP provides a detail history for each communication detail record (CDR), which includes listing all users that have listened to the recording of a call or video visitation. The detail history is easily accessible from the CDR. From the communication search results page, a user simply selects the CDR for which they would like to see the detail history and the detail history window appear to the right of the CDR. The detail history can also provide information as to users that have monitored, downloaded, tagged or added a noted to the CDR and recording.
System Logs

System Logs provide an audit trail of all user activity happening at the facility within the NextGen SCP platform. The NextGen SCP audit and tracking feature logs each user’s specific activities for investigative purposes. This activity log can be accessed by specified site administrators only or by site personnel with authorized security credentials.

The audit and tracking feature will log which recordings were monitored or played by a specific user, in addition to:

- When a user logs in to the system
- How long a user stays in the system
- What the user did with a recording
- Changes to custody accounts
- Changes to Personal Allowed Number (PAN) lists
- Changes to Global List entries
- Changes to security permissions
11. The System must provide the ability for Department staff to make notes on visits. 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™) allows authorized users to add notes and tracking numbers to communication detail records associated with recordings. This feature is accessed via the notepad icon in the communication detail record and allows authorized users to add notes—such as a tracking number, gang affiliation, duration into the call, and any other notes associated with the call—to an incarcerated communication. This feature also allows authorized users to either keep the note private to their investigation or to share the note with other users. From the Notes tab on the communication detail record, users may also view previous public notes associated with the communication.

Adding a Note to a Communication Detail Record

Authorized WA DOC users can search for notes through the Advanced Search function. This feature allows searches on the CDR tracker number, note type (no notes, my private notes, or shared notes), or keywords—such as a gang affiliation—within the CDR tracker notes. As with every report in the NextGen SCP user interface, the search results are exportable to Excel, PDF, or CSV.
12. **The System must have the ability for Department staff to restrict/suspend/terminate visitors from video visitation for specific periods of time and reverse the restriction if needed. Describe how Vendor will meet this requirement.**

Vendor’s response:

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

NextGen SCP does provide the ability to WA DOC to restrict, suspend and terminate visitors for a specific period of time and reverse the restriction if needed from the visitor contact profile page.

A notable feature of the NextGen SCP platform is the Contact Profile. Biographical information is pulled from the family & friend Securus Online account to create a unique profile for constituents requesting or having managed contact with an incarcerant, such as video visitation. This allows for a single location to view visitor information, manage their settings, apply unique rules, or suspend them individually from specific product access at the facility.

### Visitor Contact Profile Page

**Visitation Rules**

Visitation Rules allow WA DOC to set up restrictions and rules that determine the frequency of visitation by user, terminal, location, user group, and site. This feature allows authorized facility personnel to create and enforce rules, such as allowing the incarcerant user group to have a maximum of two on-site visits per week. Visitation Rules do not apply to Emergency calls.

Visitation Rules are accessed through the “Admin” menu. Select “Visit Rules” from the drop-down menu.
Creating New Visitation Rules

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

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

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

During the creation of a rule, the rule can be associated with a user, terminal, location, user group, or site. Users can create a new rule without an initial association. However, new rules will not be in effect until there is, at least, one entity associated. Associations, in order of priority, are as follows:

- **User Association:** Rule applies only to a specific Incarcerant or user
- **Terminal Association:** Rule applies to a specific terminal. This is a cumulative rule applied to the Terminal only – NOT the users under the Terminal*
- **Location Association:** Rule applies to a specific location such as a pod. This is a cumulative rule applied to the Location only – NOT the users under the Location*
- **User Group Association:** Rule applies to every member of the user group to which the rule is associated
- **Site Association:** Rule applies holistically to the Site. This is a cumulative rule applied to the site only – NOT the users under the Site*

*The behavior of cumulative rules will soon change such that the rule will apply to all users at the association level.*
Rules are also prioritized based on the association level in which they are applied. For example, a visitation rule applied to a User (highest priority) takes higher priority than a rule associated with a Site. This means that if there is a Site level rule that allows incarcerants to have one on-site visit per 1 month and a User level rule for a specific incarcerant to have five on-site visits per 1 month, the User level rule take priority.

Example Visitation Rule:

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

  **Reads:** 2 onsite visits per 1 week

If two rules with the same priority conflict, both rules will need to pass to schedule and appointment. An example of this conflict is an Incarcerant User Group visitation rule to allow one on-site visit per week and an Attorney User Group visitation rule that allows five on-site visits per week. Both rules must pass to schedule a visit.

**Associating Visit Rules**

Enforcement of a Visit Rule requires association with a user, terminal, location, user group, or site. There are two ways to associate a rule:

- From the Manage > Visits or Visitors menus
- From the Incarcerant profile page

**Editing Visitation Rules**

Editing or deleting a visit rule can be accomplished from several different pages, including:

- **Admin > Visit Rules**
- **Manage > Inmates > Visit Settings**
- **Manage > Visitors**

When editing a visitation rule, you can modify all components of the rule as well as add and delete associations. A popup showing the number of impacted sessions displays before saving a rule change. This prevents the unintentional cancellation of previously scheduled visits. If the rule change does not impact scheduled appointments, a confirmation popup will appear.
13. The System must provide the ability to search recorded visits by visitor, offender name, and offender DOC number. Describe how Vendor will meet this requirement.
Vendor’s response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Our system will allow the DOC to search recorded visits by visitor, offender name, and offender DOC number and more. Authorized WA DOC users begin by generating communication reports on all Securus Video Visitation (SVV) events through the NextGen Secure Communications Platform™ (NextGen SCP™) user interface. WA DOC users can perform a dynamic search using the single-input omnibox or an advanced search. These will allow the user to search and filter by

- Date range
- Incarcerant identifier, such as ID, PIN, and first or last name
- Communication type
- Communication status (complete or incomplete)
- Destination number (partial or full number entry)
- Call type
- Three-way or Remote Call Forwarding detected, watched status, wireless indicator, or Continuous Voice Identification
- Visitor and visit type (SVV)
- Visitor contact number
- Visitor identifier, such as first or last name, email, and visitor ID
- Per phone/terminal, per location, and per offender
- Number restriction and/or status assignment
- Broad search with no data entry
- Prepaid account number
- Destination zone (local, interLATA, interstate, intraLATA, international)
Searching for SVV Events

Advanced Search for SVV Communication Records

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

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

Vendor’s response:

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

Our customer service for video visitation issues is available 24 hours a day, 7 days a week, 365 days per year for both facility users and friends and family users.

Facility Support through Securus’ Technical Support Center

Securus provides superior customer service capabilities from a state-of-the-art operations center located in Carrollton, Texas. Securus’ Technical Support Center (TSC) is staffed by 50 support technicians 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.

Securus’ TSC serves as a single point of contact for facility staff to request service or make inquiries **24 hours a day, 7 days a week, 365 days per year** and has three convenient methods of contact:

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

The TSC uses a call distribution system to automatically manage the flow of inbound customer calls, routing 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.

Upon contact from a facility, each service request is assigned one of three initial priority levels, each with its own resolution and escalation timelines. Every effort is made to resolve the problem remotely within the designated timeframes and many service requests can be resolved during the initial request. If the service request cannot be resolved remotely, 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 which 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 the appropriate party for problem resolution. The TSC retains ownership of all service requests and is responsible for the escalation and update functions.

Securus has had more than 120 patents issued and another 70 pending patent applications, all of which are supported by our TSC. No competitor can match Securus’ TSC experience in working with corrections officials to quickly resolve and manage calling programs. Securus’ experience and technology allows us to create and manage calling
programs for corrections facilities that put top priority on providing safety and security to the public.

### Service Response Times and Escalations

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Service Priority Description</th>
<th>Response Time</th>
<th>Customer Communication Guideline</th>
<th>Escalations</th>
</tr>
</thead>
</table>
| P1             | A P1 is our highest service level which is defined as 60% or more of the functionality of the System being adversely affected by the System Event. | 4 hours       | • 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 | • 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 is defined as 30% to 59% of the functionality of the System being adversely affected by the System Event. | 12 hours      | • 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 | • 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 |
<table>
<thead>
<tr>
<th>P3</th>
<th>P4</th>
</tr>
</thead>
<tbody>
<tr>
<td>A P3 assignment is defined as 5% to 29% of the functionality of the System being adversely affected by the System Event.</td>
<td>If response is delayed, escalation procedures within Securus' Management Team are activated to ensure appropriate resources are allocated to resolve the service request.</td>
</tr>
<tr>
<td>A P4 assignment is defined as less than 5% of the functionality of the System being adversely affected by the System Event.</td>
<td>Technical Support Manager &amp; Field Service Manager.</td>
</tr>
<tr>
<td>24 hours</td>
<td>Technical Support Director &amp; Field Service Director.</td>
</tr>
<tr>
<td>Securus Technical Support Center notifies the facility when the service issue is resolved</td>
<td>VP Service &amp; Operations.</td>
</tr>
<tr>
<td>If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival</td>
<td>Securus Technical Support Dispatch or Manager &amp; Field Service Technician contacts the customer with an estimated time of arrival.</td>
</tr>
<tr>
<td>If a technician is required, Securus Dispatch or Field Service Technician contacts the customer with an estimated time of arrival.</td>
<td>Securus Technical Support Director &amp; Field Service Director.</td>
</tr>
</tbody>
</table>

**Friends & Family Support through Securus’ Friends & Family Call Center**

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. Customers can use our 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.securustech.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 to handle multi-language end user complaints.

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 addresses customer questions the first time, 99% of the time. As evidence of our continued commitment to customer satisfaction, Securus was named a three-time winner at the 2018 Stevie Awards for Sales & Customer Service.

15. Describe Vendor’s process for allowing Department staff to submit service tickets when issues arise.

Vendor’s response:

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

Securus prides itself on our customer service, and to that end we have tried to make it as easy as possible to report issues and submit service tickets by providing WA DOC with multiple methods to do so. WA DOC personnel can Submit service tickets or routine
service orders through either our Technical Support Center, through the DOC’s dedicated account manager, or through the Facility Service Request Portal.

Securus Maintenance and Technical Support Services

Service tickets can be submitted through our Securus Technical Support Center (TSC) 24 hours a day, seven days a week, 365 days per year. The TSC is a state-of-the-art operations center located in Carrollton, Texas. More than 50 technicians staff the to ensure prompt problem resolution. There are three ways to contact the TSC:

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

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.

The TSC uses a distribution system to manage the flow of inbound customer service tickets automatically routing calls directly to our support technicians in a skills-based, platform specific manner. 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. Every effort is made to resolve the problem remotely within the designated timeframes, and Securus resolves most service ticket requests during the initial request. If necessary, a field service technician is dispatched to the facility to expedite resolution.

Account Management

Washington DOC will be assigned an account manager who will be responsible for product training, monitoring system and product usage, proactive account support, account reviews, and reactive account support in order to ensure quality of service. The Securus Account Management group is a dedicated single point of contact service team that proactively manages the day-to-day needs of facilities to ensure the best possible experience from all our products, services, and support.
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

Ticket Number with Detail
16. The System must have the ability to notify customers that their account has been suspended and to provide an explanation for the suspension. Describe how Vendor will meet this requirement.

**Vendor’s response:**

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

When an authorized facility user moves to suspend a visitor a pop-up box will appear where they will be able to select the dates of suspension and also provide comments regarding the suspension. Any comments that the facility user includes will be added to the email sent to the visitor advising of the suspension.

![Suspend Visitor](image)

17. The System must ensure that public customers agree to DOC’s rules (policies) regarding use of the services. The System should require customers to affirm their understanding of these rules. Describe how Vendor will meet this requirement.

**Vendor’s response:**

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

Securus can easily accommodate customized DOC policies regarding the use of the services both at initial set up and throughout the contract. During initial implementation, our dedicated implementation team will obtain WA DOC’s policies regarding the use of video visitation and upload them into the system. Every time a public customer schedules a video visitation with an incarcerant the visitor will have to acknowledge the DOC’s terms and conditions regarding the use of video visitation. If at any time the DOC changes their...
rules or policies regarding the use of services, they would provide the new policy to their dedicated Securus Account Manager, who will provide them to the Securus Online team for upload.

Additionally, public customers can always find the policies and terms and conditions for a specific facility at the Securus Online website. Clicking on “Facilities and Pricing” under Video Product, the customer can search for the specific terms and conditions that apply to the facility where their incarcerant is located.
18. Video quality sent from the Incarcerant must be a minimum of Full HD resolution and must, at a minimum, display in that resolution. Describe how Vendor will meet this requirement.

Vendor's response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

The camera on Securus' video visitation terminal HD camera (720p @ 30 fps) with autofocus.

19. Vendor must provide Department a monthly report detailing video visitation quality including the quality of the video received by the friends and family and the quality of the video received by the incarcerant. Describe how Vendor will meet this requirement.

Vendor's response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus will provide a monthly report of reported video issues by incarcerants and friends and family regarding visitation quality.

Securus utilizes high quality video using low bandwidth. Securus video visitation is configured to H.264 video standards and provides for the following to ensure quality video:

- video transmission speeds of 64 Kbps – 2 Mbps,
- a wide range of video resolutions and bit rates, including: CIF (352 x 288 pixels), SIF (352 x 240 pixels), QCIF (176 x 144 pixels),
- supports up to 30 frames per second of high-quality video at 384+ Kbps,
- supports up to 15 frames per second of high-quality video at 64 – 320 Kbps, and
- supports both a constant or variable bit rate and frame rate.

Additionally, 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.

20. Describe Vendor's approach to handling complaints regarding video visitations and describe the circumstances under which a refund would be issued.

Vendor's response:
SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Visitors will be able to report issues regarding video visitation to Securus' Friends and Family Call Center (SFFCC). Securus has designed our US-based customer service center to handle customer inquiries and needs as quickly and efficiently as possible. We regularly
measure our performance against industry standards and our own tough expectations to ensure the highest level of service possible.

Securus is unique among its national competitors in offering an in-sourced call center located in the Dallas metropolitan area to provide customer service to friends and family members of offenders. Our call center employs approximately 150 customer service representatives who are trained and managed by Securus management.

Live agent support is available to friends and family members 7 days a week, 24 hours a day, and 365 days a year through our Securus Friends and Family Call Center (SFFCC).

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.

Also end-users may access Securus’ customer service via chat 24 hours a day, seven days a week.

Securus strives to deliver superior customer service and resolve customer issues in one call. As a source of escalation for offender’s friends and family members, call center supervisors are always available to assist customers. In general, the following escalation list may be utilized after 24 hours of not receiving a resolution for issues and/or problems. For our friends and family member end-user customers, Securus addresses customer questions the first time, 99% of the time. Certain issues and/or problems may require time to research and resolve and may take more time. A SFFCC agent will keep the external customer up to date on progress if resolution takes more time.

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

Refunds and Credits

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.

21. Describe the methodology Vendor's technicians will use in equipment testing to ensure it is properly working. Will Vendor have periodic testing or only as and when a complaint is filed by a user?

Vendor's response: SECURUS HAS READ, UNDERSTANDS, AND WILL COMPLY WITH THIS REQUIREMENT.

Securus employs approximately 224 field service associates including Regional Managers and a centralized Field Dispatch team to support our national customer base. The Field Service Technicians (FST) are strategically positioned to meet the response time requirements of our customers and reside near each customer location. Currently there are five (5) FSTs to maintain equipment in Washington State. FSTs are all required to have extensive telecommunication background and are Securus-certified to service our product offerings. The FTSs have direct access to senior technical support and engineering resources to expedite repairs and minimize customer downtime.
<table>
<thead>
<tr>
<th>Field Service Technician</th>
<th>Experience</th>
</tr>
</thead>
<tbody>
<tr>
<td>Jeff Ollar</td>
<td>• Onsite FST at Pierce County, WA</td>
</tr>
<tr>
<td></td>
<td>• Been with Securus since 9/9/2011</td>
</tr>
<tr>
<td>Brandon Jenkins</td>
<td>• Onsite FST at King County, WA</td>
</tr>
<tr>
<td></td>
<td>• Been with Securus since 9/28/2015</td>
</tr>
<tr>
<td>Kenneth Duhe</td>
<td>• Rover FST</td>
</tr>
<tr>
<td></td>
<td>• Been with Securus since 6/4/2019. He was hired specifically to support WA DOC</td>
</tr>
<tr>
<td>Russ Beecher</td>
<td>• Rover FST</td>
</tr>
<tr>
<td></td>
<td>• Been with Securus since 7/24/2017. He recently relocate within WA to be closer to WA DOC facilities.</td>
</tr>
<tr>
<td>John Phipps</td>
<td>• Rover FST</td>
</tr>
<tr>
<td></td>
<td>• Been with Securus since 3/18/2019.</td>
</tr>
</tbody>
</table>

**Quality Control Testing During Implementation**

During installation, Securus technicians will thoroughly test the system and installed hardware. Our technicians use a quality control checkpoint system at each phase of an installation:

- **Quality Control Checkpoint 1 – Provisioning:** After customer provisioning is complete, Securus technicians submit a quality control review to the Engineer, Project Manager, and Account Manager for the project. Please refer to Exhibit A for the “Provisioning Checklist,” for an example of this quality control tool.
- **Quality Control Checkpoint 2 – Pre-Installation:** While on-site, Securus Field Service Technicians complete a checklist to ensure that the physical installation characteristics meet or exceed Securus standards. Please refer to Exhibit A for the “Field Technician Checklist,” for an example of this quality control tool.
- **Quality Control Checkpoint 3 – Equipment Testing/Functional Validation:** Technicians complete test call scenarios and phone labels, call durations, on/off times, administrative terminals, and verify other customer configurations. Please refer to Exhibit A for the “Test Validation Checklist,” for an example of this quality control tool and the steps followed. Technicians will follow these equipment testing/functional validation steps whenever the review equipment and hardware.
Quality Control Checkpoint 4 – Acceptance: The Securus Project Team provides copies of all quality control documents, equipment inventory records, and network diagrams. The Securus Project Team will host a review of these documents with WA DOC. Please refer to Exhibit A for the “Customer Acceptance Checklist,” for an example of this quality control tool.

These tools are used to verify that work is completed properly before moving to the next step in a process. Customers must indicate their satisfaction with a sign off moving to the next step in a process.

Testing Procedures Post Installation

Because Securus continuously monitors all data centers, infrastructure components, platform systems, communications services, and hardware using the SolarWinds® suite of network performance monitors, our technicians will be alerted if there is an issued with the hardware. In addition to the continuous monitoring through the NOC, Securus will work with WA DOC on a maintenance schedule to review equipment, if desired.

If an issue is detected that requires on-site service, our dispatch team contacts the assigned 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.

Upon resolving the primary issue, the Field Service Technician will perform a system check to detect any unreported issues and conduct preventative maintenance checks while on-site, including:

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

Problems identified during this check are addressed by the Field Service Technician during the same visit unless additional parts are required to resolve the issue.

Upon completion of the repairs, the FST will validate problem resolution with the primary site contact and obtain sign-off on the repairs performed. After obtaining sign-off, the FST will record the transaction in our problem management system through his or her laptop.

Service Parts

Securus field service technicians maintain a working level of spare parts for minor repairs consisting of telephone sets, handsets, dials, and replacement circuit boards, either on-site
or in their truck. If a technician does not have required a part, Securus will drop-ship the item to the site. Securus will ship counter-to-counter on the same day in critical situations.

Quality

Securus sends an e-mail customer satisfaction survey to the primary site contact following each service event. Customer concerns are immediately escalated to the Regional Service Manager and the National Service Director. The Regional Service Manager is required to contact the customer within 24 hours to better understand the concern and implement a correct action plan. Securus executives review the summary of each issue along with the corrective actions on a monthly basis. Our current survey results show 94% satisfaction with Field Service with 77% indicating they were “delighted” with the service they received.

22. What kind of periodic monitoring will the Vendor perform to ensure video visits are successful? How will you ensure customer satisfaction?

Vendor’s response:

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

Securus will use a combination of remote monitoring system and our Account Management teams to make sure Securus Video Visitation is functioning optimally at WA DOC facilities at all times.

Remote Monitoring, Diagnostics, and Troubleshooting

Securus continuously monitors all data centers, infrastructure components, platform systems, and incarcerant telephone systems (ITS) 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, 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.

Our NOC is located at our headquarters in the Dallas, Texas, metro area. The NOC is staffed 24x7x365 by Securus employees who are network experts certified in the systems and software used to monitor all system functions and equipment, as well as the associated network. The NOC maintains failure reports, service history, and other diagnostic information, which are available to the DOC when requested.
Premise Equipment and Polling

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

Account Management

The Securus Account Management group is a dedicated single point of contact service team that proactively manages the day-to-day needs of facilities to ensure the best possible experience from all our products, services, and support. In addition to Natasha Samuels, WA DOC’s current Account Manager for JPay services, WA DOC will be assigned an account manager for Securus ITS, VVS, and associated services, who will be responsible for product training, monitoring system and product usage, proactive account support, account reviews, and reactive account support in order to ensure quality of service.

Quarterly Performance Reviews

Securus has assigned a dedicated account management team, which includes not only the sales and support staff, but also the DOC’s assigned Account Managers who will monitor the ongoing service and maintenance request and will conduct regularly scheduled site visits to ensure that you are receiving the highest level of customer service. In addition to these site visits, Securus offers quarterly Operational Reviews in which your Account Manager will meet with the WA DOC staff and discuss operational performance, successes, and opportunities for improvement. Securus uses the information from these meetings to improve our service delivery platform. This approach allows Securus to consistently perform at Net Promoter Scores that are among the highest recorded by any business in any industry.
## CUSTOMER ACCEPTANCE FORM

### EQUIPMENT INSTALLATION

<table>
<thead>
<tr>
<th>Description</th>
<th>Notes</th>
<th>Completed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Equipment Room - All phone equipment is professionally installed within designated areas.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Room - All phone equipment is properly labeled.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Room - All telecom and electrical wiring is mounted securely, and managed using best practices for wire/cable management.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Room - The Equipment Assignment Record has been completed and is attached to the equipment rack.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Room - All necessary equipment is grounded appropriately and using designated power sources provided by the facility.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Equipment Room - All excess equipment, trash, or other materials have been removed from the equipment room.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Installation - All phones have been installed in the correct locations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Installation - All phones have been securely mounted and inspected.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Installation - All phone handsets and keypads have been inspected</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Installation - All information placards have been installed.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Telephone Installation - All telephones have been accurately identified, and logically associated with their physical location.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workstation Installation - All workstations have been installed in designated locations.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Workstation Installation - All workstations have been used to access S-Gate UI.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

Securus Technologies, Customer Acceptance Checklist
# EQUIPMENT OPERATION

<table>
<thead>
<tr>
<th>Operation</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Phone System Operation</td>
<td></td>
</tr>
<tr>
<td>All custom prompts (tag prompts, facility name prompts) have been reviewed and confirmed.</td>
<td></td>
</tr>
<tr>
<td>Phone System Operation</td>
<td></td>
</tr>
<tr>
<td>Detainee and called party call flows have been reviewed and confirmed.</td>
<td></td>
</tr>
<tr>
<td>Phone System Operation</td>
<td></td>
</tr>
<tr>
<td>Call time limits have been reviewed and confirmed.</td>
<td></td>
</tr>
<tr>
<td>Phone System Operation</td>
<td></td>
</tr>
<tr>
<td>Call schedules have been reviewed and confirmed.</td>
<td></td>
</tr>
<tr>
<td>Phone System Operation</td>
<td></td>
</tr>
<tr>
<td>Applicable phone system features have been reviewed and verified (further defined as necessary to include all feature requirements)</td>
<td></td>
</tr>
<tr>
<td>Workstation Operation</td>
<td></td>
</tr>
<tr>
<td>Workstations have access to S-Gate UI, and user logins have been provided to necessary personnel.</td>
<td></td>
</tr>
<tr>
<td>Workstation Operation</td>
<td></td>
</tr>
<tr>
<td>S-Gate UI functionality, including reports, block/unblock, call schedules, live call monitoring, and audio download/CDRW have been tested and confirmed</td>
<td></td>
</tr>
<tr>
<td>Data Verification</td>
<td></td>
</tr>
<tr>
<td>All PIN/PAN data has been uploaded or input.</td>
<td></td>
</tr>
<tr>
<td>Data Verification</td>
<td></td>
</tr>
<tr>
<td>All blocked/free/privileged calling lists have been uploaded or input.</td>
<td></td>
</tr>
<tr>
<td>Data Verification</td>
<td></td>
</tr>
<tr>
<td>All phone locations (such as POD B, Lefl) have been correctly input into system.</td>
<td></td>
</tr>
</tbody>
</table>

## FORM VERIFICATION

<table>
<thead>
<tr>
<th>Checklist</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Field Installation Checklist</td>
<td></td>
</tr>
<tr>
<td>The Field Installation Checklist has been completed with success, reviewed, and signed by necessary parties.</td>
<td></td>
</tr>
<tr>
<td>Test / Validation Checklist</td>
<td></td>
</tr>
<tr>
<td>The Test/Validation Checklist has been completed with success, reviewed, and signed by necessary parties</td>
<td></td>
</tr>
<tr>
<td>30-Day Support Plan</td>
<td></td>
</tr>
<tr>
<td>The post-implementation support plan (acceptance criteria, SLAs, support contact, and escalation list) has been completed, and provided to appropriate customer contacts.</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Customer Contact</th>
<th>Project Manager</th>
<th>Installation Field Technician</th>
</tr>
</thead>
<tbody>
<tr>
<td>X</td>
<td>X</td>
<td>X</td>
</tr>
</tbody>
</table>

Securus Technologies, Customer Acceptance Checklist
Installation Equipment & Provisioning User Acceptance Signature Form

Site Id: 

Site Name: 

By my signature below I acknowledge I have reviewed the installation check list and I hereby confirm completion of the scope of work as required for acceptance approval which includes equipment, system functionality, and provisioning of the inmate phone system installed by Securus Technologies.

Facility Point of Contact Name: 

Printed Name: 

Signature: ___________________________ Date: ________________

Install Field Technicians assigned to installation:

Printed Name: 

Printed Name: 

Printed Name: 

Securus Technologies, Customer Acceptance Checklist
## Customer Provisioning Checklist

### Project Preparation

<table>
<thead>
<tr>
<th>Preparation</th>
<th>Project Manager - Create Install Record</th>
<th>Preparation - Project Manager</th>
<th>Preparation - Project Manager / Sales Associate</th>
<th>Preparation - Project Manager / Installation Support Team</th>
<th>Preparation - Project Manager</th>
<th>Close Preparation - Project Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Create Installation Record within Installation Project Management System: Build Install Record to include:</td>
<td>Review Contract, Master Service Agreement, and Statement of Work to identify specific project requirements, including:</td>
<td>Output Installation Record and submit to Sales Associate(s) for pre-installation review.</td>
<td>Conduct sit-down review of Installation Project, to review:</td>
<td>Lock finalized Installation Record within Installation Project Management System:</td>
<td>X Project Manager:</td>
</tr>
<tr>
<td></td>
<td>- Site Name, State</td>
<td>- Installation Scope</td>
<td>- Installation Scope</td>
<td>- Installation Scope</td>
<td>- Installation Record</td>
<td>Signature / Digital Signature Required</td>
</tr>
<tr>
<td></td>
<td>- Site ID</td>
<td>- Feature Requirements</td>
<td>- Feature Requirements</td>
<td>- Feature Requirements</td>
<td>- Signature Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Contract ID</td>
<td>- Installation Process Requirements, including timelines</td>
<td>- Installation Process Requirements, including timelines</td>
<td>- Installation Process Requirements, including timelines</td>
<td>- Digital Signature Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Billing ANI</td>
<td>- Service Level Agreements</td>
<td>- Service Level Agreements</td>
<td>- Service Level Agreements</td>
<td>- Required</td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Project Manager</td>
<td>- Recording Policy Requirements</td>
<td></td>
<td>- Recording Policy Requirements</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Field Service Manager</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Inside Support Technician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- Field Service Technician</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- AFCE Number</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>- AFCE Outlay</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>SCN CUSTOMER PROVISIONING</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>---</td>
<td>---</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Access Installation Project Management System and review Installation Record. Before proceeding, ensure all necessary information is contained within the record.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Access the SCN Customer Provisioning System  - Create Customer Record, using Customer Name, Customer State, and Contract ID  - Select the required call recording and storage profile from drop down menu  - Create Sub-Customer Record (Site), using Site Name and State  - Select appropriate time-zone from drop down menu  - Select the “Home” Data Center from drop down menu</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Access the Customer Setup WIZARD within the SCN Customer Provisioning System  - Create the MAIN, BOOKING, and DISABLED Management Port Groups (MPG)</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Select the desired MPG group from the drop down menu, and select required features and dialing instructions/restrictions from the Entitlements Section of the Customer Setup WIZARD. This includes:  - Dialing class of service, such as Collect, Debit, etc.  - Site Name Audio Announcement  - Enable PINs / PANs and PIN / PAN Length  - MPG Call Duration and Time Schedules  - Billing ANI Identification</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>INTEGRATED ACCESS DEVICE (IAD) PROVISIONING</strong></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Generate IAD Config File(s) by accessing IAD Config Generation Utility  - Enter Installation Record Number  - Enter Site ID  - Enter Site Name, State  - Choose Circuit Type (MPLS or DSL)  - Enter IAD Port Count (8/24)  - Enter Internal IP Address (from Internal IP Access list)  - Enter LEC Provided External IP  - Enter Securus Access Tag Number (from Asset Tag list)  - Save Configuration, and Click “GENERATE CONF”</td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>E-mail the IAD Config File(s) to the appropriate Field Service Technician(s). Upload IAD Config File(s) to Installation Record within Installation Project Management System. Update Installation Record to include Internal IP, External IP, and Asset Tag for the IAD(s)</td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support / Field Service</strong></td>
<td>Work with Field Technician to apply IAD Config file(s) to IAD Device(s) during the Onsite Test and Turn-up (T&amp;T) process.</td>
</tr>
<tr>
<td><strong>Provisioning – Installation Support</strong></td>
<td>Link IAD device(s) to Customer Record within SCN Customer Provisioning System.  - Select IAD Type  - Input IAD Asset Tag  - Input IAD IP Address Configuration</td>
</tr>
</tbody>
</table>

Securus Technologies, Customer Provisioning Checklist
| Review – Project Manager / Installation Support Team Supervisor / Engineer | Review Customer and Site Provisioning within the SCN Customer Provisioning System. Review Installation Record within Installation Project Management System. Validated Feature Requirements listed in the Installation Record match the features and configurations established in the SCN Customer Provisioning System. Validate IP Scheme, IAD Config, and Network | ☐ |
| Review – Project Manager / Installation Support Team | Conduct sit-down review of Installation Project, to review: -Installation Scope -Feature Requirements -Installation Process Requirements, including timelines -Service Level Agreements | ☐ |
| Review Manager | Lock finalized Installation Record within Installation Project Management System. | ☐ |
| Close Review – Project Manager | Finalize and Lock Customer and Site Provisioning | Signature / Digital Signature Required |

Project Manager

Installation Support Team Supervisor

Engineer

Securus Technologies, Customer Provisioning Checklist
<table>
<thead>
<tr>
<th>Review Item</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Does the equipment received match the equipment listed on the Sales Order? Please include equipment receipt checklist with returned survey.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Was all of the equipment received without damage?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is any additional equipment required to complete project? Please include equipment request form for any additional equipment.</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Site Inventory</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Equipment Location and Security</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there sufficient HVAC in the phone room?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the equipment in a secure location?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the physical condition of the phone room satisfactory?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there evidence of any construction occurring in or around the phone room?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there adequate perimeter space around the phone equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Electrical</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is a grounded, dedicated circuit being used to power the equipment?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there a secondary power source available in the phone room?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the equipment grounded with a #12 green insulated copper wire?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the equipment utilizing a UPS unit or building UPS?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the UPS plugged into the Towermax KSU?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is the Towermax KSU installed correctly, and electrically grounded?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there lightning protection installed on the T1/C.O. side of the system?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is there lightning protection installed on the station side of the system?</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Network / Telecom</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all lines/circuits been identified, tagged, and terminated? Please include circuit/line inventory.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all lines/circuits been tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the modem line and BTN been installed and tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all routers, channel banks, and IADs installed and visible on the network? Please include updated network diagram.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Is all wiring cleanly installed, utilizing wire management systems and recommend best practices? Please include pictures of all phone room wiring.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has all network and telecom cabling been tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Review Item</td>
<td>Result</td>
<td>Notes</td>
</tr>
<tr>
<td>---------------------------------------------------------------------------</td>
<td>--------</td>
<td>-------</td>
</tr>
<tr>
<td>Have all inmate phones been installed and securely mounted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are all the conduit, pedestals, and backboards securely fastened?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have the new placards been installed in every phone?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all of the phones been tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all of the phones been identified with a logical port ID and facility port location?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have all of the port assignments been setup in the SCN Customer Record?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Have the phones been associated with the correct management port groups?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the on-off times and call timers set?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Are the TDD phones installed and securely mounted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has a successful TDD to TDD call been tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has a successful TDD to relay station call been tested?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Data Upload / Migration

- Has PIN information been obtained from previous system and provided to Installation Support Team for import?
- Has blocked/free/privileged calling list information been obtained from previous system and provided to Installation Support team for import?

### Test Plan / Customer Acceptance and Approvals

<table>
<thead>
<tr>
<th>Review Item</th>
<th>Result</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Has the test plan been completed with success?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the Project Manager and Engineer reviewed and accepted?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Has the customer acceptance form been reviewed and accepted?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

---

**Facility Installer**

**Secondary Reviewer**
# TEST / VALIDATION CHECKLIST

<table>
<thead>
<tr>
<th>Facility Name</th>
<th>Installer Name:</th>
</tr>
</thead>
<tbody>
<tr>
<td>State:</td>
<td>Ticket Number:</td>
</tr>
<tr>
<td>Main Address:</td>
<td>Date:</td>
</tr>
<tr>
<td>Contact Name</td>
<td></td>
</tr>
</tbody>
</table>

**LEGEND**

- ✓ Satisfactory/Complete
- X Unsatisfactory
- No Mark = Not Reviewed

### Data Validation

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Verify phone numbers are correct.</td>
<td></td>
</tr>
<tr>
<td>Verify phones are associated with correct MPS.</td>
<td></td>
</tr>
<tr>
<td>Verify call times are set correctly.</td>
<td></td>
</tr>
<tr>
<td>Verify call duration is set correctly.</td>
<td></td>
</tr>
<tr>
<td>Verify all <code>$&lt;</code> prefix numbers have been input into system.</td>
<td></td>
</tr>
<tr>
<td>Verify PSRN data has been input into system.</td>
<td></td>
</tr>
<tr>
<td>Verify initial 5-Digit user accounts have been reset.</td>
<td></td>
</tr>
</tbody>
</table>

### Test Cases

<table>
<thead>
<tr>
<th>Test Case</th>
<th>Notes</th>
<th>1</th>
<th>2</th>
<th>3</th>
<th>4</th>
<th>5</th>
<th>6</th>
</tr>
</thead>
<tbody>
<tr>
<td>Go offshore on telephone and check for voice prompts.</td>
<td></td>
<td>1</td>
<td>2</td>
<td>3</td>
<td>4</td>
<td>5</td>
<td>6</td>
</tr>
<tr>
<td>Assess English and Spanish language to validate call times.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform hands-on check on telephone.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Verify product acceptance test call.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform test call and verify correct facility key log in place.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform test call and verify that system prompts you for your name.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform test call and verify that both parties are notified of monitoring and recording.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Send private test call and verify test call is not monitored or recorded.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform local collect test call, select rate, and validate the rate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform domestic I.D. collect test call, select rate, and validate the rate.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Perform International Direct test call (NPA/704-4145).</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Site-Feature Set Testing

<table>
<thead>
<tr>
<th>Site-Feature Set Testing</th>
<th>Workstation ID</th>
</tr>
</thead>
<tbody>
<tr>
<td>Test Case</td>
<td>Notes</td>
</tr>
<tr>
<td>5-Digit connectivity tested.</td>
<td></td>
</tr>
<tr>
<td>6-Digit login successful.</td>
<td></td>
</tr>
<tr>
<td>Perform live call monitoring test.</td>
<td></td>
</tr>
<tr>
<td>Listen to audio recordings to ensure audible recordings.</td>
<td></td>
</tr>
<tr>
<td>Test ISDN/voice/data number list maintenance.</td>
<td></td>
</tr>
<tr>
<td>Perform POTS data entry.</td>
<td></td>
</tr>
<tr>
<td>Disable/Enable incoming phones through softphone function.</td>
<td></td>
</tr>
<tr>
<td>Perform call delay exercises.</td>
<td></td>
</tr>
<tr>
<td>Perform call recording download.</td>
<td></td>
</tr>
<tr>
<td>Test CD burning for call recordings.</td>
<td></td>
</tr>
</tbody>
</table>

**Additional Site-Specific features added as necessary**

---

### Signature

- Project Manager: [Signature]
- Installer/Support Technician: [Signature]
- [Signature]
- [Signature]