

Wireless Containment Solution .....	1
I. Wireless Containment Solution .....	1
E. Outbound Facility WCS Telephone Number .....	2
II. Control of Information.....	2
III. WCS Maintenance and Accountability .....	3
A. WCS Maintenance .....	3
B. WCS Accountability.....	3
IV. WCS System Controls .....	3
B. Planned Outage of WCS .....	4
C. Emergency Outage .....	4
V. Emergency Services – 911 .....	4
VI. Managed Access Experience .....	5
VII. References .....	5
VIII. Action.....	5
Attachments .....	6

<b>Section-04 Security</b>	<b>OP-040122</b>	<b>Page: 1</b>	<b>Effective Date: 12/09/2021</b>
<b>Wireless Containment Solution</b>	<b>ACA Standards: None</b>		
<b>Scott Crow, Director Oklahoma Department of Corrections</b>		<b>Signature on File</b>	

## **Wireless Containment Solution**

The Oklahoma Department of Corrections has contracted with Securus Technologies, Inc. (Securus) to provide technology that will aid the agency in controlling the unauthorized use of contraband cell phones. This technology is called Wireless Containment Solution (WCS) and is a proprietary service offered by Securus.

### **I. Wireless Containment Solution**

- A. WCS is managed access for wireless communication services. Through the cooperation of the wireless services providers, Securus maintains up to the minute wireless communication frequencies and reproduces the signals to direct wireless devices in range to go through a managed network that functions much like the networks in the public domain.
  
- B. Devices operating from within the Securus WCS network are blocked from being able to access the public wireless services networks unless the device is on an authorized list of wireless devices. The only authorized devices that will be allowed on the authorized list will be as listed below. No others will be permitted unless authorized by the chief of Operations.
  - 1. Authorized list of wireless devices.
    - a. Agency director;

- b. Chief of Operations;
  - c. Chief of Staff;
  - d. Chief of Technical Services;
  - e. Chief administrator of Institutions;
  - f. Administrator of Institutions;
  - g. Facility warden;
  - h. Facility deputy warden;
  - i. Facility chief of security;
  - j. Facility correctional health services administrator; and
  - k. Administrator of Technology and Logistics Operations.
- C. Administrators listed in section I. B. item 1. of this procedure, and others placed on the approved list, will only be able to make outbound calls. No inbound calls, or data packets, including texts, will pass through the system to the phone.
- D. All outbound calls, including texts, will be captured by the system and will show in reporting systems which are reviewed at several levels of the agency. Outbound calls will not show in caller ID as the callers originating number. The system captures the call and processes all outbound calls as one telephone number specific to each facility.
- E. Outbound Facility WCS Telephone Number
- Oklahoma State Penitentiary (918) 820-4131

## II. Control of Information

Devices that are captured by the WCS network are monitored by the Securus NextGen Secure Communications Platform (NGSCP), which is the system that manages all information produced by Securus applications, such as the inmate telephone service. User access to the WCS application is controlled through the super admin of the NGSCP platform. Access to the WCS application can only be granted by the agency director, chief of Operations, inspector general, deputy inspector general, chief of Technical Services, or administrator of Technology and Logistics Operations.

- A. The inspector general and designees will have full investigative access to the WCS system.
- B. The agency director, chief of Operations, chief of Technical Services, and the application owner will have NGSCP WCS administrative capability will have access any available widgets and permissions.
- C. The warden at the facility containing an active WCS installation shall receive the following permissions.
  - 1. WCS permissions in NGSCP
    - a. System status widget;
    - b. Peak days widget; and
    - c. Peak hours widget.

### III. WCS Maintenance and Accountability

#### A. WCS Maintenance

- 1. Securus is responsible for all maintenance on WCS components, to include any preventive maintenance required.
- 2. The agency is responsible for daily visual inspections of WCS components and any issues noted should be reported to Securus WCS team via the Securus account manager.

#### B. WCS Accountability

- 1. The facility warden will provide documentation upon request to the chief administrator of Institutions of the daily visual inspection of the following: WCS servers and hardware in main storage room and WCS components throughout the facility. Daily visual inspections of the WCS equipment will be documented on the "Shift Supervisor's Daily Report" ([Attachment B](#)) of [OP-040102](#) entitled "Master Roster and Post Order Guidelines" and the shift supervisor's post log.
- 2. Securus will be responsible for maintaining cameras assigned to their equipment and alarms attached to their equipment allowing for early warning of tampering or issues. Information from cameras and alarms will be available to ODOC as necessary to complete investigations or other inquiries.

### IV. WCS System Controls

A. The WCS system in the main storage area will be equipped with a kill switch. The kill switch will be in the immediate area of the WCS server racks and will be contained inside a red lockable box. Facility warden, deputy warden, chief of security, and shift supervisor will be informed of exact location of the kill switch and the key that unlocks the kill switch box. The facility is responsible for providing a lock on the kill switch box with the key being an emergency key which will be secured in the key managed access storage cabinet (Key Watcher) or other emergency key location.

B. Planned Outage of WCS

If the agency director or inspector general, or designees, need to schedule a planned outage of the WCS system at the facility, the Securus WCS team will be notified by phone call to the Securus WCS Network Operations Center (NOC) at 1-972-277-0600, with written notification to the chief of Operations and chief of Technical Services.

1. Planned outages can be directed to specific areas of the facility.
2. Only preauthorized agency personnel will be accepted at the Securus NOC. The inspector general is responsible with informing the chief of Technical Services any changes to the authorized list to contact the Securus NOC.

C. Emergency Outage

In an emergency, the chief administrator of Institutions or chief of Operations may order the immediate suspension of the WCS system by instructing the facility warden to turn off the WCS kill switch. The facility warden will call WCS Network Operations Center (NOC) at 1-972-277-0600 and state the following:

1. "This is 'STATE YOUR NAME'. We have turned the WCS OFF at 'FACILITY NAME and LOCATION. Please let the appropriate WCS personnel know."
2. To enable the WCS, turn the switch back on and inform the Securus NOC. Turning the switch on immediately restores the WCS system.
3. Shutting off the system with the kill switch effects the entire facility WCS.

V. Emergency Services – 911

A. Calls that originate from within the WCS containment area will be directed to the local 911 Emergency Communications Center (911 ECC). In the event that the 911 ECC determines the call is not within the scope of an

emergency, the call will be forwarded to the facility emergency number. The facility warden is responsible for keeping the 911 ECC informed of any changes to this number.

- B. Each facility will maintain on file or attempt to enter into a memoranda of understanding (MOU) between the facility warden and the commander of the 911 ECC.
- C. The facility warden will be responsible for making yearly contact with the 911 ECC to renew the MOU and ensure information is current.
- D. Each facility with a WCS will maintain this file in the warden's office for review and compliance verification.

VI. Managed Access Experience

When a mobile device, under the managed access of the WCS, makes a call, the WCS plays an automated announcement informing the calling party that the call can not go through. This announcement is customizable. Changes to this greeting can only be made through the administrator of Technology and Logistics Operations.

VII. References

Policy Statement P-040100 entitled "Security Standards for the Oklahoma Department of Corrections"

OP-040102 entitled "Master Roster and Post Order Guidelines"

VIII. Action

The chief of Technical Services will be responsible for compliance with this procedure and for the annual review and revisions.

Any exception to this procedure will require prior written approval from the agency director.

This procedure will be effective as indicated.

Replaced: None. This is a new procedure.

Distribution: Policy and Operations Manual  
Agency Website

Attachments

Title

Location

[Attachment B](#)

“Shift Supervisor’s Daily Report”

[OP-040102](#)