



Kern County Sheriff's Office

Policies and Procedures

TITLE: CELLULAR COMMUNICATION DEVICES			NO: J-1900
APPROVED: Donny Youngblood, Sheriff-Coroner			
EFFECTIVE: October 9, 1992	REVIEWED: October 4, 2023	REVISED: October 4, 2023	UPDATED: October 4, 2023

POLICY

The Kern County Sheriff's Office maintains agency-issued cellular communication devices for the purpose of enhancing the law enforcement mission and conducting official business when regular telephones and computers are not readily available. A cellular communication device may also be utilized to provide superior communications in the management of field or special operations.

Employees assigned a cellular communication device shall ensure the safety of the equipment from theft, damage, and unauthorized use. Failure to care for the equipment may result in disciplinary action and reimbursement for the cost of its replacement or repair.

Employees shall have no expectation of privacy in any communication created, received, or sent using the Sheriff's Office-issued device. Employees shall not assume that communications or messages of any type are confidential because a private password is used. Electronic communications are "public records" under Government Code sections 7922.570-7922.585 and may be subject to disclosure under California law. In addition, all employees will be in compliance with the County's Electronic Communications Usage Policy.

DEFINITION

CELLULAR COMMUNICATION DEVICE: Is any portable communication device that is designed to be carried by a person to connect to a telecommunications network in order to transmit and receive voice, video, or other data. The devices may include mobile telephones and smartphone devices, similar wireless two-way communication devices, tablets, and any other portable devices with the capability to connect to a globally connected network system (i.e., the internet).

DIRECTIVE A –CELLULAR COMMUNICATION DEVICE ISSUANCE

As a general rule, depending on assignments and the needs of the position, a cellular communication device will be issued only to Sheriff's Office personnel whose official duties necessitate the use of the requested device. The following assignments are examples of jobs that require the issuance of a cellular communication device:

- Management personnel with full-time responsibility for a section, division, or bureau of the Sheriff's Office.
- Supervisory personnel who require a cellular communication device to maintain contact with their subordinates in order to provide effective supervision.
- Personnel assigned to specialized units that entail duties requiring the enhanced communication capabilities provided by a cellular communication device.
- Field assignments requiring the use of a body worn camera.

Lieutenants or civilian managers of other units who believe their personnel's duties require the use of a cellular communication device may contact the Technology Services Section (TSS) Manager to authorize the issuance of a cellular communication device.

DIRECTIVE B – CELLULAR COMMUNICATION DEVICE RETURN

Employees whose official duties no longer necessitate the use of a cellular communication device shall return the device, along with all issued accessories, only to the TSS and without delay. Cellular communication device accessories may include the charger and protective case. The employee shall ensure the cellular communication device is physically clean and reset to factory settings.

DIRECTIVE C – CELLULAR COMMUNICATION DEVICE PROTECTION

The following protocols shall apply to all Sheriff's Office-issued cellular communication devices:

- All cellular communication devices shall be carried in the approved carrier/case issued by the TSS.
- All cellular communication devices that access any Kern County Sheriff's Office systems are required to be password protected and approved by the TSS Manager.

EFFECTIVE: October 9, 1992	REVIEWED: October 4, 2023	REVISED: October 4, 2023	UPDATED: October 4, 2023
---	--	---	---

DIRECTIVE D – MOBILE DEVICE MANAGEMENT

All Sheriff's Office devices will be managed by our internally owned Mobile Device Management (MDM) solution. This will allow the Sheriff's Office to maintain FBI/CJIS security compliance. The MDM is used to set policies as well as monitor device update levels. All settings implemented by the MDM are a direct result of the FBI/CJIS security policy.

- Employees are prohibited from downloading third-party applications to their devices. If an employee would like to install a third-party application, they will need to seek approval from their lieutenant or civilian manager via the chain of command. If approval is granted, then a TSS helpdesk ticket will need to be opened. TSS will then verify that the third-party application will not compromise Sheriff's Office data or conflict with FBI/CJIS security policy. If the third-party application is determined to be safe to install, TSS will deploy the approved application to the requested device(s). The ticket will need to include the approving lieutenant/civilian manager, which device(s) it needs to be installed on, and the purpose for the requested third-party application.
- Employees are responsible for updating the software on their cellular communication devices. TSS will send out email reminders to staff whose device(s) are not up to date. Failure to update a device can result in service disruption or device lock out. If an employee needs assistance updating a device, they can open a TSS helpdesk ticket.

DIRECTIVE E – CELLULAR COMMUNICATION DEVICE USAGE

As a cost savings measure, the TSS will periodically collect an overview usage of assigned cellular communication devices to ensure the Sheriff's Office is not funding cellular plans for devices that are not being regularly used by the assigned employees. The TSS will consult with Section managers to determine if unused or minimally used devices need to remain assigned to their employees or returned to the TSS.

EFFECTIVE: October 9, 1992	REVIEWED: October 4, 2023	REVISED: October 4, 2023	UPDATED: October 4, 2023
---	--	---	---