



KAY IVEY
GOVERNOR

State of Alabama Department of Corrections

Alabama Criminal Justice Center
301 South Ripley Street
P. O. Box 301501
Montgomery, AL 36130-1501
(334) 353-3883



JOHN Q. HAMM
COMMISSIONER

April 22, 2025

**ADMINISTRATIVE REGULATION
NUMBER**

353

**OPR: COMMISSIONER'S
OFFICE**

MOBILE DEVICES

I. GENERAL

This Alabama Department of Corrections (ADOC) Administrative Regulation (AR) establishes the authorization of Mobile Device(s) inside any ADOC facility and supports searches of facilities and offenders to control contraband and its disposition. The ADOC reserves the right to investigate, retrieve and read any communication or data stored on its respective servers, and that which is composed, transmitted or received through ADOC voice services. This policy aims to ensure the security and integrity of ADOC operations, prevent the introduction of unauthorized devices into secure environments, and maintain accurate records of mobile device usage by employees and contractors.

II. POLICY

The ADOC will only allow mobile devices authorized by the Commissioner inside any/all correctional facilities. Possession and/or use of cellular phones and/or Mobile Device(s) on premises are prohibited. These devices are monitored and identified for security purposes. Communications made from any unauthorized operational devices by an employee, contractor, volunteer, inmate, or visitor shall be identified. Violation of this regulation will result in penalties as allowed by law. Wireless devices and communications authorized by the Commissioner are exempt.

III. DEFINITIONS AND ACRONYMS

- A. **Authorized**: A mobile device is authorized if it has been explicitly approved by the Commissioner of the ADOC for official, operational, or emergency use.
- B. **Command Staff**: Executive leadership personnel generally comprised of the Commissioner/designee, Deputy Commissioner(s), Assistant Deputy

Commissioner, Institutional Coordinator(s), Warden(s), Directors, and Captain(s).

- C. **Commercial Frequency Two-Way Radios**: Digital or analog radios operating on frequencies assigned to commercial communications companies. These radios may have cell phone capability. They differ from radios that operate on public safety frequencies.
- D. **Pager**: Small personnel radio receiver that gives an indication when a radio signal is received.
- E. **State-Issued Mobile Device(s)**: Any state-issued or state-owned device(s) that allows the user to access, store, and transmit information wirelessly to include text messaging, internet access, data, or any form of communication.
- F. **Mobile Device(s)**: Any device or device(s) that allows the user to access, store, and transmit information wirelessly to include text messaging, internet access, data, or any form of communication.
- G. **Unauthorized**: A mobile device is unauthorized if it has not been explicitly approved by the Commissioner, or if it is used for prohibited purposes.

IV. **RESPONSIBILITIES**

- A. The Commissioner's Office is responsible for:
 - 1. Authorizing the possession of mobile devices within any ADOC facility, either directly or through an appointed designee.
 - 2. Issuing official approval or termination letter(s) or delegating that responsibility to an authorized appointee via a formal appointment letter.
 - 3. Ensuring the appointed designee(s) adhere to all ADOC policies, operational guidelines, and documentation procedures for approvals and terminations.
- B. Special Services is responsible for:
 - 1. Maintaining a Digital Repository: Maintain a secure digital repository of all mobile device authorizations. This repository should be regularly updated to ensure accurate and accessible records.
 - 2. Reporting Discrepancies: Shall notify the Commissioner of any discrepancies related to mobile device authorizations.

- C. The IT Division is responsible for:
1. Creating and Maintaining Identification Cards: Creating and maintaining identification cards for personnel who are authorized by the Commissioner.
 2. Maintaining Mobile Device Registrations: Maintaining accurate mobile device registrations through ADOC Form 353-B, *Device Registration Form*.
 3. Providing Technical Support and Troubleshooting: Providing ongoing technical support for mobile devices, including troubleshooting issues related to device functionality and registration.
- D. The Warden or designee(s) are responsible for:
1. Monitoring Authorized ADOC Form 353-B, *Device Registration Form*: Monitoring and ensuring the proper handling and submission of the authorized ADOC Form 353-B, *Device Registration Form*, for mobile device use.
 2. Ensuring Compliance with Policies and Procedures: Ensuring that all staff members comply with ADOC policies and procedures, particularly regarding mobile device use, security protocols, and documentation.
 3. Reporting Discrepancies: Responsible for notifying the Special Services Deputy Commissioner of any discrepancies related to mobile device authorizations, usage, or other security concerns.
- E. Approved Mobile Device user(s) are responsible for:
1. Updating Device Information: Must follow proper procedures for updating their device information, including, but not limited to, registering new devices, even if the phone number remains the same
 2. Completing Required Documentation: Completing all required documentation, ensuring all sections are accurately filled out and submitted for final approval.
 3. Adhering to Device Usage Policies: Comply with all applicable policies and guidelines regarding the appropriate use of mobile devices, including restrictions on unauthorized usage within secure or restricted areas.
 4. Maintaining Device Security: Maintaining the security of their devices, ensuring that they are password-protected, and reporting any lost or stolen devices immediately.

5. Notifying Chain of Command Immediately: Any change to the device, phone number, or information submitted during the authorization process must be reported immediately to their direct chain of command and updated with Special Services and IT.
6. Reporting Discrepancies: Must notify the appropriate authority (e.g., Special Services or the IT Division) of any discrepancies, issues, or irregularities related to their device or device registration.
7. Refraining from Unauthorized Devices: Must ensure that only approved devices are used within the facility and are prohibited from bringing any unauthorized devices into the ADOC or other secure environments.
8. Compliance with Monitoring Procedures: Must be aware that their devices may be subject to monitoring or audits and must comply with any monitoring procedures as outlined in organizational policies.
9. Cooperation with Security Audits: Responsible for cooperating fully with any security audits related to mobile devices and providing requested information in a timely manner.

F. Unapproved Mobile Device user(s) are responsible for:

1. Refrain from Bringing Unauthorized Devices: Prohibited from bringing any unauthorized devices into the facility or other secure areas.
2. Compliance with Mobile Device Policies: Comply with all applicable ADOC policies and procedures regarding the use of mobile devices, including the restriction on using devices that have not been approved
3. Cooperation with Security Measures: Must cooperate with any security measures or audits related to unauthorized devices, including providing requested information.
4. Adhering to Restricted Area Guidelines: Must ensure that no unauthorized device is brought into secure or restricted areas within the facility, adhering to all applicable safety and security protocols.
5. Powering Down Devices: If an unauthorized device is inadvertently brought into a secure area, users must immediately power down the device to minimize any security risks or breaches.

V. PROCEDURES

- A. Appointee Oversight: The Commissioner or Commissioner's Office appointed designee is responsible for reviewing all mobile device requests

and issuing approval or termination using official templates. The designee must ensure that:

1. All approvals or terminations are documented and stored in the digital repository managed by IT and Special Services.
2. Any change in mobile device details after approval is promptly updated in the system.
3. The requester is instructed to immediately notify their chain of command if their device, number, or submitted details change at any point.

Initial Security Checkpoint: Upon arrival at the first security checkpoint, mobile device users must disclose the type(s) of devices they are bringing into the facility and display the device identifiers by dialing *#06#.

Facility staff will verify whether the devices are authorized for entry into the facility.

Once verified, facility staff will complete ADOC Form 353-B, *Device Registration Form*, and securely attach it to the mobile device user's ADOC picture ID or government-issued identification card.

- B. Exit Security Checkpoint: Upon exiting the facility, the device and the information on ADOC Form 353-B, *Device Registration Form*, will be re-examined to ensure the device being taken out of the facility is the same device that entered.

Whenever possible, the same staff member who conducted the initial security check should perform the exit examination to ensure consistency.

- C. Responsibility for Device Accountability: Mobile device users are responsible for always maintaining the accountability and security of their devices while inside the facility.
- D. Immediate Reporting of Unauthorized Devices: Any unauthorized or illegal devices detected must be immediately reported to Special Services (LESD, K9, etc.).

If an unauthorized device is tied to a specific offender or found in common areas, the number of devices must be documented in the summary section of the Incident Reports application.

Confiscated unauthorized devices deemed contraband will be processed according to LESD evidence and contraband management procedures.

- E. Device Examination and Documentation (Entry): Upon arrival at the first security checkpoint, facility staff will examine the Mobile Device(s) being brought into the facility. The Mobile Device user(s) shall disclose the type(s) of device(s) and display the device's identifiers by dialing *#06# to verify the information.
- F. Responsibility for Device Accountability: The Mobile Device user is responsible for always maintaining the accountability and security of their wireless device(s) while inside the facility, ensuring the device remains properly tracked and accounted for.

Facility staff will confirm whether the device(s) are authorized for entry. After the examination, the facility staff conducting the first security check will complete ADOC Form 353-B, *Device Registration Form*.

The completed form will be securely attached to the Mobile Device user's ADOC picture ID or government-issued identification card for tracking purposes.

- G. If applicable, Device Re-examination (Exit): When the employee exits the facility, facility staff will re-examine the device and verify the information on ADOC Form 353-B, *Device Registration Form*, to ensure that the device being taken out of the facility is the same device that entered.

Whenever possible, the same facility staff member who examined the device upon entry should perform the exit examination to ensure consistency and accuracy in tracking the device.

- H. Immediate Reporting of Unauthorized Devices: Any occurrence involving the detection or discovery of unauthorized or illegal wireless devices must be immediately communicated to Special Services (e.g., LESD, K9, etc.).

This includes situations where a device can be linked to a specific offender, as well as instances where a device cannot be directly linked to an offender but is found in common areas of the facility.

- I. Incident Reporting: The number of unauthorized or illegal devices found must be documented in the summary section of the Incident Reports application. Any confiscated unauthorized or illegal phones that are deemed contraband must be processed according to LESD evidence/contraband management processes.
- J. Warden/designee is responsible for: Preventing Contraband Introduction: The Warden/designee is responsible for ensuring the prevention of contraband, including unauthorized wireless devices, from entering the facility. This includes overseeing security measures, staff adherence to protocols, and

ensuring proper checks and documentation are followed to prevent contraband from being introduced.

VI. DISPOSITION

Any forms used will be disposed of and retained according to the Departmental Records Disposition Authority (RDA).

VII. FORMS AND ANNEXES


- A. ADOC Form 353-A, *Mobile Communication Device Access Request*
- B. ADOC Form 353-B, *Device Registration Form*
- C. ADOC Form 353-C, *Device Registration Approval Letter*
- D. ADOC Form 353-D, *Device Registration Termination Letter*
- E. ADOC Form 353-E, *Commissioner's Appointee Designation Letter*
- F. Annex A to AR 353, *Device Security Procedures*
- G. Annex B to AR 353, *Device Security Operation Guidelines*

VIII. SUPERSEDES

This Administrative Regulation is a new policy.

IX. PERFORMANCE

- A. Code of Alabama 1975 § 14-1-1.1 *et seq.*



John Q. Hamm
Commissioner

Attachments:

Attachment A to AR 353, *Secure Area Sign*

Attachment B to AR 353, *Contraband Sign*

ALABAMA DEPARTMENT OF CORRECTIONS
MOBILE COMMUNICATION DEVICE ACCESS REQUEST



Seq # _____

Requestor Information

Name _____ Title _____
Facility _____ Employer _____

Device Information

Type _____ Make _____ Model _____
IMEI _____ IMSI _____ Phone # _____

Justification Information

Decision Information

Approved ☐ Denied ☐

Commissioner's Signature

Date Signed

ALABAMA DEPARTMENT OF CORRECTIONS

DEVICE REGISTRATION FORM



353-B Device Registration Form

353-B Device Registration Form

This form collects mobile device information. Please submit a new form if any information changes. Please also resubmit if any changes, like new device, even if the number for the device stays the same.

Section 1

Device Owner's information

1. First Name *

Enter your answer

2. Last Name *

Enter your answer

3. Are you an employee of ADOC? *

☐ Yes

☐ No

4. Who is your employer? *

Enter your answer

5. What is your position? *

Enter your answer

6. Who is the point of contact for your employer? (A supervisor or co-worker, cannot be yourself) *

Enter your answer

7. What is the point of contacts phone number? *

Enter your answer

8. Please provide employee number. (If number is not known, please provide last 5 of social) *

Enter your answer

ADOC Form 353-B
04-2025

ALABAMA DEPARTMENT OF CORRECTIONS
DEVICE REGISTRATION APPROVAL LETTER



DATE

To: [Employee/Contractor Full Name]

Position: [Insert Position Title]

Facility: [Insert Facility Name]

Subject: Approval for Mobile Device Use within ADOC Correctional Facility

Dear [Employee/Contractor Last Name],

This letter serves as official approval for your use of a mobile device within the secured grounds of the Alabama Department of Corrections (ADOC) [Insert Facility Name]. This authorization is granted under the authority of Commissioner John Hamm or his appointed designee and is contingent upon your strict adherence to all policies and procedures governing electronic device usage in a correctional setting.

Your device may be used solely for official ADOC business purposes. Any misuse or violation of departmental security protocols may result in immediate revocation of this authorization and potential disciplinary action.

You are required to immediately notify your direct chain of command and update the ADOC Form 353-B if your device, telephone number, or any submitted information changes. Failure to do so may result in revocation of authorization.

Please ensure that a copy of this approval letter is maintained on your person while within the facility and shared with facility security staff upon request.

Sincerely,

[Full Name]

[Title]

For: Commissioner John Hamm
Alabama Department of Corrections

ALABAMA DEPARTMENT OF CORRECTIONS
DEVICE REGISTRATION TERMINATION LETTER



DATE

To: [Employee/Contractor Full Name]

Position: [Insert Position Title]

Facility: [Insert Facility Name]

Subject: Termination of Authorization for Mobile Device Use within ADOC Facility

Dear [Employee/Contractor Name],

This letter serves as formal notice that your authorization to use a mobile device within the secured grounds of the Alabama Department of Corrections (ADOC) [Insert Facility Name] is hereby **terminated**, effective immediately.

This decision has been made under the authority of Commissioner John Hamm or his appointed designee and may be due to (but not limited to) changes in job duties, reassignment, voluntary withdrawal, non-compliance with ADOC policies, or expiration of your previously approved device registration.

As of the date of this notice, you are no longer permitted to bring in or use any personal or previously registered mobile device within any secure area of the ADOC facility. Any further use or possession of such devices without renewed written approval will be considered a violation of ADOC policy and may result in disciplinary action or legal consequences.

Please ensure your device registration form (ADOC Form 353-B) is updated accordingly, and any associated documentation is returned or disposed of per facility guidelines.

Should you have questions regarding this termination or if you believe it was issued in error, please contact your direct supervisor or facility security office.

Sincerely,
[Full Name]
[Title]

For: Commissioner John Hamm
Alabama Department of Corrections

ALABAMA DEPARTMENT OF CORRECTIONS
COMMISSIONER'S APPOINTEE DESIGNATION



DATE

By Authority of the Commissioner
State of Alabama

Be it known that: [Insert Full Name],

[Insert Position Title], of [Insert Facility/Location], is hereby appointed and vested with the authority to serve as a Commissioner's Appointee for the sole purpose of overseeing and approving the use of mobile and electronic devices within the secured facilities of the Alabama Department of Corrections (ADOC).

By this designation, and under the authority granted to the Commissioner of the Alabama Department of Corrections, the above-named individual is empowered to evaluate, authorize, and revoke permissions related to mobile device usage by ADOC personnel and approved contractors in accordance with established departmental policies and procedures.

This authority is strictly limited to:

1. Approval or termination of device use within ADOC secure areas
2. Oversight of compliance with ADOC Form 353-B
3. Enforcement of departmental policy regarding electronic devices in correctional environments

This appointment shall remain in effect until formally amended, revoked, or superseded by the written order of the Commissioner or his designated authority.
Issued under my hand and seal, this [Insert Day] day of [Insert Month], [Insert Year].

By Order of the Commissioner:

John Q. Hamm
Alabama Department of Corrections

ALABAMA DEPARTMENT OF CORRECTIONS

DEVICE SECURITY PROCEDURES



The following procedures are established to ensure strict control, accountability, and integrity of mobile devices authorized for use within ADOC correctional facilities:

A. Access Control

1. **Authorized Personnel Only** – Access to secure areas with mobile devices is limited strictly to personnel with written approval from the Commissioner or his designated appointee.
2. **Verification at Checkpoints** – Upon entry and exit, all mobile devices must be declared and verified using IMEI or other identifying information (*#06#). Entry and exit data must match without deviation.

B. Device Inspection

1. **Physical Inspection** – All mobile devices must be physically inspected by facility staff at designated checkpoints to ensure compliance with registration and approval documentation.
2. **Documentation Verification** – Staff shall confirm the ADOC Form 353-B and match the registered data with the physical device. Any inconsistency is grounds for denial of entry and subject to report.

C. Incident Response

1. **Unauthorized Devices** – Discovery of an unauthorized device will be treated as a **contraband incident** and immediately reported to Special Services (LESD, K9, or designated authority).
2. **Chain of Custody** – Confiscated devices must be secured and processed according to LESD evidence handling protocols, including submission into the contraband tracking system.

D. Compliance Audits

1. **Random Inspections** – Facility staff and internal auditors may conduct unannounced inspections to verify mobile device usage compliance.
2. **Audit Cooperation** – All staff must comply with audit and inspection protocols, including providing devices, identification, and documentation upon request.

ALABAMA DEPARTMENT OF CORRECTIONS

DEVICE SECURITY OPERATIONAL GUIDELINES



The following guidelines govern the authorized use, handling, and accountability of mobile devices to support the operational security and functionality of ADOC personnel:

A. Authorization Protocol

1. **Written Approval Required** – No mobile device may be brought into any ADOC secure facility without written authorization from the Commissioner or designee.
2. **Appointment Authority** – The Commissioner may assign a ranking official (Command Staff level or higher) to act as an approving authority.

B. Usage Standards

1. **Official Use Only** – Authorized mobile devices are to be used **exclusively** for ADOC-related duties. Personal use is prohibited.
2. **Restricted Areas** – Use of mobile devices in restricted zones (e.g., segregation units, control rooms, armories) is prohibited unless explicitly permitted for mission-specific duties.

C. Accountability Measures

1. **Registration Required** – All authorized devices must be registered using ADOC Form 353-B and linked to the user's identification credentials.
2. **Device Control** – Users must maintain positive control of their devices at all times. Devices shall never be left unattended or shared.

D. Change Notification

1. **Immediate Reporting** – Any changes to the authorized mobile device (IMEI, phone number, replacement unit) must be reported immediately to the user's chain of command and updated with Special Services and IT.
2. **Documentation Update** – Users are responsible for submitting an updated ADOC Form 353-B reflecting any changes and securing continued authorization.



SECURE AREA

CONTRABAND PROHIBITED:

Only items authorized by the ADOC Commissioner are allowed.

LEAVE UNAUTHORIZED ITEMS IN YOUR VEHICLE:

Ensure devices are powered down and locked in your vehicle.

YOU ARE SUBJECT TO SEARCH AND/OR ELECTRONIC MONITORING.



ALABAMA DEPARTMENT OF CORRECTIONS
CONTRABAND SIGN

