Augusta University
Policy Library

Augusta University Owned Cellular Devices Policy
Policy Manager: Chief Information Officer

POLICY STATEMENT
Augusta University (AU) issues AU-owned cellular devices and service plans (including FirstNet where applicable) to support University business and emergency response/continuity. Devices must be requested, used, secured, monitored, and returned to protect University Data, control costs, and meet AU, BOR, and USG requirements.

WHO SHOULD READ THIS POLICY
This policy applies to all AU faculty, staff, students (including graduate assistants), affiliates, contractors, volunteers, and other authorized users issued an AU-owned cellular device or AU-owned cellular service (including FirstNet) for University business, regardless of manufacturer, operating system, provider, or location (on/off campus, travel, or remote work).

AFFECTED STAKEHOLDERS
Indicate all entities and persons within the Enterprise that are affected by this policy:

☒ Alumni ☒ Faculty ☒ Graduate Students ☒ Health Professional Students
☒ Staff ☒ Undergraduate Students ☒ Vendors/Contractors ☐ Visitors
☐ Other:

DEFINITIONS
These definitions apply to these terms as they are used in this policy:

- **Cellular Service Plan**: Voice, text, data, and any add-on features (e.g., hotspot data, international roaming) associated with an AU-owned cellular device and billed to AU.
- **Emergency Responder / Critical Personnel**: Authorized and trained AU personnel whose job duties include emergency response, incident management, life safety, continuity of operations, or other mission-critical functions and who may be eligible for FirstNet service or other priority communications as approved by AU.
- **FirstNet**: A nationwide wireless broadband network intended for public safety communications that may provide priority and preemption capabilities for eligible users during incidents.
- **Limited Incidental Personal Use**: Minimal personal use that does not interfere with work, does not result in cost, and complies with AU and USG acceptable use and security requirements.
- **Mobile Device Management (MDM)**: AU-approved technology used to enroll, configure, secure, monitor, and (when necessary) remotely lock or wipe AU-owned cellular devices.

- **Records / Open Records**: Communications, images, files, texts, call logs, or other information related to AU business may constitute University records and may be subject to records retention requirements and lawful requests under the Georgia Open Records Act.

- **Sensitive Electronic Information / Sensitive Data**: University Data that is confidential or regulated and requires protection from unauthorized access, use, disclosure, alteration, or loss. Examples include PHI, PII, PCI data, confidential/proprietary institutional data, certain financial/audit information, and other data protected by law or policy (e.g., HIPAA/HITECH, PCI-DSS, Georgia Open Records Act exceptions).

- **University Data**: Any data created, received, maintained, transmitted, or stored to conduct AU business, regardless of format.

PROCESS & PROCEDURES

1. **Device Assignment and Registration**
    - All AU-owned cellular devices must be obtained through AU Information Technology (IT) and enrolled in AU-approved Mobile Device Management (MDM) prior to issuance, unless an exception is approved in writing by the VP Information Technology & CIO.
    - AU IT administers the AU-owned mobile device program end-to-end.
    - Departments must not purchase AU-owned mobile devices or cellular service directly outside AU IT's process; costs are billed back to units per the AU IT Procurement Policy and applicable USG requirements.
    - Each issued device must be assigned to an individual user (or documented shared-use group), recorded in AU inventory/asset records, and acknowledged by the user. Users are responsible for physical safeguarding of the device, keeping it charged and operational, and reporting issues promptly.

2. **Permitted Use**
    - Limited incidental personal use is permitted if infrequent, does not interfere with work, complies with law/policy, and does not result in cost to AU. Devices are issued for a documented, non-compensatory business need and are not additional compensation; consistent with IRS Notice 2011-72, qualifying limited incidental personal use is generally a non-taxable de minimis fringe benefit.
    - Users must comply with applicable AU/BOR/USG requirements and all applicable laws.
    - Users should have no expectation of privacy when using AU-owned cellular devices or AU services. AU may access, preserve, use, and disclose device content and usage as permitted by law and policy for operational, security, audit, investigation, records retention/open records, litigation hold, and other legitimate University purposes.

3. **Security and Data Protection**
    - Protect University Data by using encryption and AU-approved secure methods for storage/transmission. Access/handle Sensitive Data only through AU-approved apps/services; do not disable or bypass controls; and install OS/app updates promptly as directed by AU IT.
    - Report lost, stolen, detained, or suspected-compromised devices immediately to AU IT (72Cyber) and your supervisor/department so AU can take protective actions (e.g., locate, lock, wipe, and/or suspend service).
    - Use Wi-Fi/Bluetooth/hotspot features only when needed and in a way that does not expose University Data; use heightened caution when traveling.

4. **Incident Response**
    - Users issued FirstNet devices (or designated as emergency responder/critical personnel) must keep the device available for contact and response as required by their role (generally 24x7x365 except during approved leave), subject to applicable safety, legal, and location-specific restrictions.

5. **Device Maintenance and Support**
    - Users must exercise reasonable care and follow AU IT support/repair instructions for troubleshooting, warranty service, replacement, and accessory return.

6. **Compliance**
    - Compliance may be verified through audits, billing/inventory reviews, and security monitoring by AU IT and AU IT Cybersecurity. Users and departments must cooperate with audit and investigative requests.

7. **Prohibited Use**
    - Using the device for unlawful activity, harassment, threats, or any activity that violates AU/BOR/USG policies.
    - Storing or transmitting Sensitive Data using unapproved apps, accounts, or services.
    - Installing software or apps that are unlicensed, malicious, or not permitted by AU IT standards.
    - Using the device in a manner that results in excessive or avoidable cost to AU (e.g., non-business international roaming without approval).

8. **Billing, Cost Control, and Plan Management**
    - Use cost-saving features when feasible (e.g., AU-approved Wi-Fi calling/networks) and avoid non-business charges; coordinate all line/plan changes (adds, suspensions, cancellations, transfers) through AU IT. Avoidable or excessive personal charges may require reimbursement per departmental procedures.
    - Coordinate any allowance, stipend, or reimbursement for personal mobile service with AU Human Resources/Payroll in advance to ensure proper tax and documentation treatment.

9. **Travel and International Use**
    - When traveling, apply Security and Data Protection requirements with heightened caution (public charging stations, public Wi-Fi, unknown peripherals) and report any loss, theft, detention of equipment, or suspected compromise immediately so AU can take protective actions (e.g., remote wipe and account disablement).

10. **Return of Devices, Reassignment, and Separation**
    - Maintain physical control until handed to AU IT (or an authorized departmental custodian). If immediate return is not possible (e.g., remote location), contact AU IT for approved return/shipping instructions.
    - University Data on AU-owned devices is AU property. Do not factory reset/wipe or remove data before return.
    - Phone numbers are AU assets and will not be ported to personal accounts/devices at separation. Any port/transfer is prohibited unless expressly approved in writing by the VP Information Technology & CI and department leadership and completed through AU-approved procedures.
    - Return AU-owned devices to AU IT for secure decommissioning (e.g., account removal and wipe/sanitization) and required records preservation/retention. Return the device and accessories (e.g., charger, case; SIM/eSIM details when applicable) as-is unless AU IT instructs otherwise; if feasible, keep the device powered on to support timely deprovisioning.

11. **Exceptions**
    Exceptions to this policy (including exceptions from MDM enrollment or required security configuration) must be documented and approved in advance by VP Information Technology & CIO and the requesting department leadership. Approved exceptions must specify scope, duration, compensating controls, and review date. Some exceptions may also require USG-level review/approval un the USG IT Handbook.

ROLES AND RESPONSIBILITIES

- Supervisors/Departments: Approve and justify business need; ensure funding; review billing; ensure timely return upon role change/separation; and support compliance with training and policy requirements.
- Division of Information Technology (AU IT): Administer the AU-owned mobile device program (procurement coordination, provisioning, carrier management, inventory, MDM, support, and decommissioning) and ensure contract compliance.
- AU IT Cyber Security: Define security standards: review exceptions and submit for approval; support incident response; and conduct security monitoring and compliance validation.

- Emergency Management/CEPAR: Identify emergency responder/critical personnel needs and coordinate requirements for FirstNet and other incident communications capabilities.

Non-compliance
Failure to adhere to this policy may result in disciplinary action, up to and including termination of employment, as well as other administrative actions as appropriate. Sanctions may also include suspension, limitation, or revocation of access to AU's computing environment, applications, networks, and data. To protect University Data and resources, AU may also take immediate protective actions (e.g., remotely lock or wipe a device and/or suspend cellular service).

REFERENCES & SUPPORTING DOCUMENTS
Intentionally left blank.

RELATED POLICIES

- Augusta University Policy Library
- AU Acceptable Use of Information Technology Policy
- AU Data Management & Classification Policy
- AU Electronic Data Retention Policy
- AU Cybersecurity Training Policy
- Augusta University International Travel Policy
- Augusta University IT Procurement Policy (technology procurement approval process; submit requests through ServiceNow and obtain AU IT review/approval before purchase)
- Board of Regents Policy Manual (Information Security)
- USG Information Technology Handbook (key sections on access control, acceptable use, incident response, data classification, and endpoint management)
- USG Business Procedures Manual (BPM) Section 12 (Data Governance and Management)
- IRS Notice 2011-72 (tax treatment of employer-provided cell phones; IRC § 132 (fringe benefits))
- Georgia Open Records Act (O.C.G.A. § 50-18-70 et seq.)

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 5/19/2026

President, Augusta University Date: 5/20/2026