Augusta University
Policy Library

Mobile Device Policy
Policy Manager: Chief Information Officer

1.0 POLICY STATEMENT
Augusta University (AU) is committed to fostering a secure, productive, and inclusive academic and administrative environment. To support the university's academic, clinical, research, and administrative missions, AU requires that all mobile devices accessing organizational systems or data adhere to defined security controls. This policy mandates the appropriate protection of university information technology on both AU owned and personally owned devices, ensuring compliance with federal and state regulations, contractual obligations, and organizational security requirements.

This policy adheres to or exceeds the standards found in the University System of Georgia (USG), IT Handbook.

2.0 AFFECTED STAKEHOLDERS
This section identifies the groups and individuals who are expected to follow this policy when they are granted access to AU's network and have access to AU organizational data.

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

3.0 DEFINITIONS
This section defines key terms used in this policy to support consistent understanding and application.

AU-owned mobile devices: A mobile device owned and managed by the organization, and that may be used to access organizational resources.

Personally owned devices: A mobile device that is owned and managed by an individual rather than the organization, and that may be used to access personal and/or organizational resources.

Additional definitions are provided in the *Cybersecurity Charter, Appendix B*. This can be found online in the Augusta University Policy Library.

4.0 SCOPE
This section describes where this policy applies, including the types of data formats, systems, and environments covered.

This policy applies to all mobile devices that access AU resources, including but not limited to smartphones, tablets, laptops, portable hard drives, SD Cards, wearable devices, flash drives, and any portable computing or communication equipment.

5.0 ROLES AND RESPONSIBILITIES

This section assigns and documents ownership for mobile device security tasks and policy obligations, ensuring clear accountability across workforce members and the Division of Information Technology (IT).

Abstract: This section defines accountability for securing mobile devices and AU data by outlining the responsibilities of workforce members and IT for secure configuration, approved use, and timely reporting. It clarifies required user behaviors and IT operational duties that support consistent, compliant mobile device security across the university.

5.1. All workforce members:

- 5.1.1 Must ensure devices meet minimum security requirements **detailed in section 6.2 of this policy**, to include but not limited to up-to-date operating systems, passwords, authentication, encryption, and antivirus software.
- 5.1.2 Must use AU-approved third-party software for accessing organizational information.
- 5.1.3 Must maintain physical control of devices and not leave them unattended when traveling domestically or internationally.
- 5.1.4 Must ensure sensitive or confidential information is not displayed or accessed in public spaces where it may be viewed by unauthorized persons.
- 5.1.5 Must report any suspected violations or non-compliance with this policy to AU Cyber Defense or 72CYBER@augusta.edu.

5.2. The Division of Information Technology (IT):

- 5.2.1 Implement and manage device policies and configurations.
- 5.2.2 Develop and implement processes to appropriately acquire, test, deploy, and validate device patches and updates.
- 5.2.3 Detect and document anomalies that may indicate malicious activity or deviations from policy and procedures.
- 5.2.4 AU reserves the right to monitor, audit, and log activity on devices accessing AU systems.

6.0 REQUIREMENTS

This section establishes the enforceable requirements that govern how mobile devices may be used to access, store, transmit, or process AU data and systems.

Abstract: This section establishes the minimum acceptable use and security controls required for mobile devices that access AU systems or data, regardless of ownership or location. It details baseline safeguards—including encryption, authentication, configuration management, travel expectations, and incident reporting—to reduce risk to university information.

6.1 Acceptable Use

- 6.1.1 All AU owned mobile devices used to conduct the business of the organization must meet the security standards outlined in this policy and all other applicable policies.
- 6.1.2 AU has the right to approve or deny the use of a personal device in the workplace.

6.1.3 All AU owned mobile devices must adhere to the standards outlined in the *AU Encryption Policy*.

6.1.4 All mobile devices used to store, transmit, process, or access organizational restricted and/or regulated information must be owned or managed by the organization. Mobile devices not managed or owned by AU should not be used to download or store university data.

6.1.5 Jailbroken, rooted, or otherwise modified devices are **prohibited** from accessing AU systems.

6.1.6 Only approved applications will be installed on AU-owned mobile devices. AU may choose to revoke access to any or all organizational applications from a user's personal device if deemed appropriate.

6.1.7 All AU owned mobile devices must be properly cleansed or wiped in accordance with AU standards prior to donation, surplus, trade-in, redistribution, or disposal.

6.1.8 Responsible use of "Bring Your Own Devices (BYOD): The organization reserves the right to limit or revoke BYOD access if risks to data confidentiality, integrity, or availability are identified.

6.2 Security Requirements

All mobile devices that connect to the AU network or other entity on behalf of AU, regardless of location or ownership **must:**

6.2.1 Must have safeguards installed to prevent malware infection or unauthorized access to the organization network or data.

6.2.2 Adhere to password and authentication requirements as outline in AU policies and standards.

6.2.3 Use organization issued and installed data encryption software to prevent unauthorized disclosure.

6.2.4 Never be left unattended and always remain within positive control of the custodian.

6.2.5 In accordance with AU standards, every device must be wiped before ownership is transferred.

6.2.6 Have an inactivity timeout threshold no greater than 15 minutes configured.

6.2.7 Be configured with current AU baseline configurations, including Mobile Device Management (MDM) solutions such as JAMF for MacOS and iOS, System Center Configuration Manager (SCCM) and Intune for Windows OS, and limited Intune support for Android. Deviations from the baseline configurations must be authorized by the VP for Information Technology & Chief Information Officer.

6.3 Travel Requirements

6.3.1 Domestic travelers should exercise vigilance and always maintain security of their assigned AU device while traveling.

6.3.2 All mobile devices taken out of the US shall adhere to the standards outlined in the AU International Travel Policy.

6.4 Incident Reporting Requirements

6.4.1 Workforce members with custodial responsibilities for the mobile device must complete the Lost/Stolen Equipment Report, describing the device's data contents.

6.4.2 The workforce member with custodial responsibilities for the mobile device, must assist with lost/stolen device investigation, device recovery, device wiping, and breach investigation as applicable.

6.4.3 The Cyber Defense Department shall report all incidents of compromised data to the Organization Privacy Office for analysis and/or action.

7.0 COMPLIANCE

This section explains how compliance with this policy is managed, including how to request documented exceptions and the potential consequences of non-compliance.

Exceptions: If compliance with this policy is not feasible or technically possible, or if deviation from this policy is necessary to support a business function, System Owners/Data Owners (or other responsible entities) shall request a documented exception through the AU Cyber Defense (GRC) Exception to Policy (ETP) process (ServiceNow Knowledge Base Article KB2300201). All approved exceptions shall have a defined expiration date and shall be reviewed periodically for continued necessity.

Exception conditions: Failure to adhere to the conditions outlined in an approved exception to policy may result in revocation of the exception.

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 action as appropriate. Sanctions may also include suspension, limitation, or revocation of access to AU's computing environment, systems, applications, networks, and organizational data.

8.0 REFERENCES & SUPPORTING DOCUMENTS

This section lists external regulations, frameworks, USG requirements, and AU supporting resources that inform or support this policy.

NIST Special Publication 800-124, Guidelines for Managing and Securing Mobile Devices in the Organization
NIST Special Publication 800-164, Guidelines on Hardware-Rooted Security in Mobile Devices
University System of Georgia (USG) Information Technology (IT) Handbook
Service Now Knowledge Base Article, KB2300201

9.0 RELATED POLICIES

This section lists internal policies, standards and resources that inform or support this policy.

Cybersecurity Charter Policy
Acceptable Use of Information Technology Policy
Electronic Data Storage Policy
Electronic Back up Policy
Encryption Policy
Information Configuration Standards Policy
International Travel Policy
Password Protection Policy
Breach Notification – Protected Health Information Policy

All AU Policies can be found online at the Augusta University Policy Library.

APPROVED BY:
Executive Vice President for Academic Affairs and Provost, Augusta University
Date: 6/25/2026

President, Augusta University Date: 7/8/2026