1. Scope

This policy defines standards and restrictions regarding State-Issued or Personal mobile devices that connect to infrastructure, and/or access or store information owned by the State of North Carolina (NC). Mobile devices include but are not limited to smartphones, tablets, e-readers, portable media devices, and wearable computing devices. Laptop computers are outside the scope of this document. All individuals who utilize State of NC information technology (IT) resources are responsible for adhering to the following policy.

2. Responsibilities

Role	Definition
Agency Management	The Agency Head, the Agency Chief Information Officer (CIO), the Agency Chief Information Security Officer (CISO), or other designated organizational officials at the senior leadership level within the Agency are assigned the responsibility for ensuring that the goals and requirements of this policy are met. Responsible for ensuring that the approved administrative and technical privacy controls are in place and effective and for educating employees about their responsibilities.
Information System Owner	The information system owner is the individual responsible for the overall procurement, development, integration, modification, or operation and maintenance of the information system. Develops and maintains the system security plan in coordination with information owners, the system administrator, the information system security officer, and functional “end users.”
System Administrator	The System Administrator is an individual or group responsible for setting up and maintaining a system or specific system elements, implements approved secure baseline configurations, incorporates secure configuration settings for IT products, and conducts/assists with configuration monitoring activities as needed.
Agency Security Liaison	The Agency Security Liaison is responsible for ensuring that security risks are managed in compliance with the State’s requirements by collaborating with organizational entities. Liaisons are responsible for ensuring that the appropriate controls are in effect for Agency information systems.
User	A user is an approved State employee, contractor, or visitor who is authorized to conduct the business of the State.

3. Policy

3.1. State-Issued Mobile Devices

State-Issued mobile devices include all mobile devices provided by State Agencies to their users, including those purchased with State funds through a State cellular account. Within each State Agency, it is the responsibility of Agency Management to establish a process for the request and approval of State-Issued mobile devices.

Agency System Administrators are responsible for configuring State-Issued mobile devices in accordance with Statewide Information Security Policies and Mobile Policy Security Technical Implementation Guides (STIGS). All State-Issued mobile devices should be managed through an enterprise Mobile Device Management (MDM) solution if technically feasible.

3.2. Personal Mobile Devices

Within each State Agency, it is the responsibility of Agency Management to establish a process to approve and monitor the use of Personal mobile devices that connect to State Infrastructure or access/store State data. The approval process must include a legitimate business justification. All approved Personal mobile devices should be managed through an enterprise Mobile Device Management (MDM) solution or Mobile Application Management (MAM) solution.

Users must also adhere to the following technical standards and best practices:

- Use of strong passcodes and Multi-Factor Authentication (MFA)
- Regular updates of Operating Systems (OS) and applications, enabling automatic updates where possible
- Controlling application permissions to location, microphone, and camera access
- Avoid connecting to public Wi-Fi networks
- Turn off Bluetooth and Wi-Fi when not in use

Connection of Personal mobile devices to State Infrastructure is a privilege and can be revoked at any time for any reason.

3.3. Guest Network Access

Guest networks are segmented from State data and are intended to provide internet access to visitors. Prior to receiving guest access, users must acknowledge applicable terms and conditions. These may include acceptable use requirements, restricted actions, and notification of monitoring or recording activities.

4. Device Loss or Theft

Users are responsible for exercising extra care to preclude the compromise, loss, or theft of mobile devices, especially during travel.

In the event that a device is compromised, lost or stolen, users are responsible for immediately reporting the loss or theft using their Agency's incident response process and in accordance with the State's incident response process (See Statewide Incident Response Policy, IR-6 - Incident Reporting). Agency procedures should include communication with the associated Endpoint Management team to ensure appropriate media sanitization actions occur in a timely manner.

5. Records Management

All communications on State-Issued or approved Personal mobile devices are subject to the requirements of the NC Department of Natural and Cultural Resources. Within each State Agency, it is the responsibility of Agency Management to establish a process to ensure that appropriate media sanitization actions take place in accordance with Statewide Information Security Policies. Additionally, approved Personal mobile devices are subject to legal holds and public records requests.

6. Enforcement

Violations of this policy or failure to implement provisions of this policy may result in disciplinary action up to and including termination, civil litigation, and/or criminal prosecution.

Policy Approval and Review

Name	Reason	Date
Bernice Russell-Bond	Policy Update	03/02/2026