Mobile Device Management Policy

Document No.
SCIO-SEC-321-00

Effective Date	Review Date	Version	Page No.
00/00/00	00/00/00	1	1 of 8

1. Scope

This policy provides the State's security policy statements and commitment to develop, implement, and maintain information security plans to protect information and critical resources from a wide range of threats in order to ensure business continuity, and to minimize business risk for information systems and data of which the State is considered the owner. This policy applies to all State employees, contractors, and all other users of State information and information systems that support the operation and assets of the State. Use by local governments, local education agencies (LEAs), community colleges, constituent institutions of the University of North Carolina (UNC) and other executive branch agencies is encouraged to the extent allowed by law.

The requirements described in this policy apply to all mobile information systems operated through a centralized State technology group or operated independently within an agency or by external service provider. Information systems, as defined per NIST SP 800-53, are the discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

2. Responsibilities

All individuals who utilize State of NC information technology (IT) resources are responsible for adhering to this policy.

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."
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 a visitor who is authorized to use the IT system to conduct the business of the State.

3. Policy

Mobile devices, such as smartphones and tablet computers, are important tools for the organization and their use is supported to achieve business goals. However, mobile devices can also represent a significant risk to the security of the network and data if the appropriate security controls and procedures are not implemented. If not carefully managed, mobile devices can be a conduit for unauthorized access to the network, which can subsequently lead to data leakage, breaches, and network compromise. Within each State agency and/or component, the determining authority and responsibility for issuance of mobile devices network access shall rest with the Agency CIO or designee.

Mobile devices may include systems owned or operated by other components (e.g., external organizations, vendors, etc.). Agencies have the option to prohibit the use of any type of external system or prohibit the use of specified types of external systems, (e.g., prohibit the use of any external system that is not State owned or prohibit the use of personally owned systems).

State employees and authorized personnel, e.g., contractors, that have received authorization from the Agency CIO, or designee, may use approved personally owned and state-issued mobile devices to access the State network for emails and solely to conduct official State business. This requirement does not apply to users who connect to the State network through a State-supplied “guest” Wi-Fi network. Access to the State network is also extended to the State-managed wireless network (not “guest”). All mobile devices that synchronize with State e-mail or connects to the network and/or hold State data will be managed through an enterprise mobile device management solution. Mobile devices will be configured in accordance with the Statewide Information Security Policies and Mobile Policy Security Technical Implementation Guides (STIGS).

3.1. Roles and Responsibilities (User)

All users covered by this policy must acknowledge and adhere to the following requirements for mobile devices connecting to the State infrastructure:

- Users must only access data on their mobile device(s) that is essential to their role. The access and download of data classified as Confidential per N.C.G.S. 132 is strictly prohibited, unless approved by the Agency CIO or designee.
- Users must immediately report all lost or stolen devices 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). **Note:** Agencies must also report their lost or stolen devices to the Enterprise Security and Risk Management Office (ESRMO) via the Statewide Cybersecurity Situation Report.
- If a user suspects that unauthorized access to State data has taken place via a mobile device, the user must report the incident 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).

- Devices must not be "jailbroken" or have any software/firmware installed which is designed to gain access to functionality not intended to be exposed to the average user.
- Users must not download or install pirated software or illegal content onto their devices.
- Applications must only be installed from official platform-owner approved sources. Installation of code from un-trusted sources is forbidden.
- Users must prevent the storage of Restricted or Highly Restricted State data in unapproved applications on the device.
- Users must not connect devices to the State Network unless the device is compliant with State security policies and has up-to-date and enabled anti-malware protection (as applicable) or has a State approved mobile management tool installed.
- Devices must be encrypted in compliance with the Statewide Information Security Manual's compliance standards. Refer to the State's System and Communications Protection Policy, SC-13 – Cryptographic Protection control.
- Users must exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.

3.2. Roles and Responsibilities (System Administrators)

System administrators supporting approved mobile devices connecting to State infrastructure are responsible for the following:

- Device registration and asset management to include offboarding/decommissioning.
- Wi-Fi Internet access configuration. This service is limited to the State Network. Device registration is required. Personal email will not sync when connected to the State Network. State Agencies that are not managed by the NC Department of Information Technology (DIT) should develop internal policies that conform to State policy.
- Removing devices not compliant with State policies and secure configuration standards.
- Provisioning devices with endpoint protection applications, such as the following:
  - Data Leak Prevention (as applicable)
  - Malware protection
  - Encryption
  - Remote wiping/erasing of reported lost or stolen devices. Only State data will be wiped from devices when using Mobile Application Management.
- Enabling devices to access web-based applications as needed.

- Providing access control of mobile devices to Restricted or Highly Restricted data.
- Restricting which applications may be installed through whitelisting (preferable) or Blacklisting.

4. Personal Mobile Devices or Bring Your Own Device (BYOD)

Personal Mobile Devices are not authorized to connect to the State Network unless there is a justified business need and prior approval is obtained from the respective Agency CIO or designee. This does not include the use of Guest wireless networks which are a segmented portion of the State Network. Personal Mobile Devices that receive prior approval to connect may only access Agency services that they are authorized to access. Individuals will need to use the Microsoft Outlook application to access State email on mobile devices.

All users should note that connection to the State Network is a privilege and not a requirement. Additionally, Personal Mobile Devices that are used for State purposes, are subject to legal hold, a process that is used to preserve potentially relevant information when litigation is pending or reasonably anticipated.

As a condition for personally owned device connections, the device owner must accept or Opt-In to the State's mandatory security requirements. There are, however, exceptions to the level of coverage and support given to personal devices. Specifically, the user is responsible for the following:

- Settling any service or billing disputes with their telecommunications carrier
- Purchasing any required software not provided by the manufacturer or telecommunications carrier
- Device registration with the vendor and/or service provider
- Maintaining any necessary warranty information
- Battery replacement due to failure or loss of ability to hold a charge
- Backing up all personal data, settings, media, and applications in case remote wipe controls are enforced
- Installing software updates/patches
- Malware protection, e.g., anti-virus
- Device registration with DIT Unified Communications
- Installing software updates
- Reporting lost or stolen device immediately
- Reporting replacement of new devices
- Complying with the Statewide Data Classification and Handling Policy
- Complying with the Statewide Acceptable Use Policy (AUP)

4.1 Provisioning Personally Owned Devices

State employees who have a business need to access, store, or transmit State data from personally owned devices must agree to the following:

- Obtain approval from immediate supervisor and Agency CIO or designee.
- Read and sign the Agency's Acceptable Use Policy.
- Authorize the download of the State-managed mobile device management tool(s), e.g. Mobile Application Management.

5. Mobile Device Security Configurations

Users shall ensure that Restricted or Highly Restricted data is not transmitted from a non-approved mobile device. Approved secure email or collaboration services will be utilized in such cases.

- The device operating system software will be kept current.
- The device will utilize a minimum 4-digit Personal Identification Number (PIN). The device may employ physical authenticators, or biometrics to authenticate user identities or, in the case of multi-factor authentication (MFA), some combination thereof.
- The device will have a time out of inactivity that is 15 minutes or less.
- The State data on the device will be removed after 10 failed logon attempts.
- The device will be configured to encrypt content using FIPS 140-2 approved encryption.
- The device will be configured to compartmentalize State data from personal data.
- User must agree to random spot checks of device configuration to ensure compliance with applicable Statewide Information Security Policies.
- Security Configuration Baseline for supported Microsoft applications using Mobile Application Management (MAM) is located in **Appendix A**.
- See **Appendix A** for minimum supported operating system versions for android and iOS devices

6. Data Sanitization

Mobile devices that do not comply with the following requirements will be wiped or not authorized to access, store, or transmit State data:

- Device is lost, stolen, or believed to be compromised.
- Device is jailbroken.
- Device inspection is not granted in accordance with this policy.

- Device belongs to a user that no longer has a working relationship with the State, i.e. user decides to un-enroll from the Mobile Device Policy and Management solution.
- Devices that are unassigned or re-assigned as part of offboarding/onboarding procedures.

7. Records Management

All communications on State-Issued, State-maintained or approved personal mobile devices authorized for use on the State Network are subject to the requirements of the NC Office of Records Management. Personally owned devices are subject to records management requirements only where official State Data is involved.

8. 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
DocuSigned by: James Weaver 372C8D237F5547A...		3/29/2021 | 4:56 PM EDT

Appendix A

Security Configuration for Mobile Application Management

Application Protection Policy

Feature	**Selection**
Applicable Applications	PowerPoint, OneDrive, Dynamics CRM for Tablets, Teams, OneNote, Excel, Power BI, SharePoint, Word, Planner, **Outlook**, Skype for Business, Dynamic CRM for Phones
Prevent Android/iTunes/iCloud backups	Yes
Allow App to transfer data to other apps	Policy Managed Apps
Allow App to receive data from other apps	All Apps
Prevent Save As	Yes
Select which storage services corporate data can be saved to	OneDrive for Business & SharePoint
Restrict cut, copy and paste with other apps	Policy Managed Apps with paste in
Encrypt App Data	Yes
Disable app encryption when device encryption is enabled	No
Disable Contacts Sync	No
Disable Printing	No
Require PIN for App Access	Yes
Number of attempts before PIN reset	5
PIN Length	4
Allow Fingerprint or Facial recognition instead of PIN (Android 6.0+/iOS 8+)	Yes
Disable app PIN when device PIN is managed	No

Appendix A

Security Configuration for Mobile Application Management

Require corporate credentials for access	No
Block managed apps from running on jailbroken or rooted devices	Yes
Recheck the access requirements after (minutes)	15
Offline grace period (minutes)	120
Offline interval (days) before app data is wiped	90
Block screen capture and Android Assistant	Yes
Require minimum Android Version	Yes
Android/iOS Version	N-1
Require minimum App Version	Yes
Require only approved Client Apps	Yes