Office of State Human Resources

ROY COOPER
Governor

BARBARA GIBSON
Director, State Human Resources

TO: Committee and Subcommittee Chairs Listed in N.C.G.S. 143-162.5
Joint Legislative Oversight Committee on Information Technology
Fiscal Research Division
Office of State Budget and Management

FROM: Blake Thomas, General Counsel and Temporary Legislative Liaison, Office of State Human Resources

DATE: October 1, 2024

RE: Annual Report on OSHR Mobile Device Usage

In accordance with N.C.G.S. 143-162.5, the Office of State Human Resources (OSHR) submits the following report on the use of mobile devices as of October 1, 2024.

1. Any changes to agency policies on the use of mobile devices.

OSHR has adopted a new mobile device policy, which is attached to this report.

2, 3, 4, and 5. The number and types of new devices issued since the last report, the total number of mobile devices issued by the agency, the number of each type of mobile device issued, and the total cost for each type.

MOBILE DEVICE TYPE	CURRENT NUMBER OF MOBILE DEVICES	COST OF MOBILE DEVICES - ANNUAL	NEW AND DISCONNECTED DEVICES: NET NUMBER ADDED OR DISCONNECTED
Smartphone	15	$7,198.20	3 fewer
Tablet	2	$911.76	2 fewer
MiFi	19	$8,661.72	12 fewer
ANNUAL TOTAL	**36**	**$16,771.68**	**17 fewer**

The number of mobile devices decreased over the last year, as shown above. Where employees needed devices, they were reassigned from other personnel. Therefore, there were no net new devices.
Note that these figures may vary from what was listed in past reports, because it was discovered that some devices assigned to OSHR were erroneously rolling into the Department of Administration report instead of being listed for OSHR. Through agency collaboration between DIT billing, the DOA CIO, and the OSHR CIO, these errors have been corrected.

NORTH CAROLINA Office of
State Human Resources

MOBILE DEVICE POLICY (MDP)

OSHR:	Office of State Human Resources
Issued By:	Christine Hofer, OSHR Chief Information Officer
Approved By:	**Glenda Farrell, OSHR Chief Deputy**
Effective Date:	**October 1, 2024**

INTRODUCTION

PURPOSE

The Office of State Human Resources (OSHR) recognizes that mobile devices, such as smartphones, MiFi devices and tablet computers, are strategic assets of the State of North Carolina and must be treated and managed as valuable resources to carry out OSHR's mission. The purpose of this policy is to establish minimum appropriate and acceptable requirements regarding the deployment and use of mobile devices, comply with applicable state law and other rules and regulations, and establish management and reporting procedures of mobile devices.

OWNER

OSHR Chief Information Officer

SCOPE

This policy applies to the Office of State Human Resources (OSHR) employees, contractors and all other OSHR users of State information and information systems that support the operation and assets of the State. The requirements described in this policy apply to all mobile device and mobile information systems operated through a centralized State technology group or operated independently within OSHR or by an external service provider.

POLICY

Mobile devices 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. The determining authority and responsibility for issuance of network access for mobile devices shall rest with the OSHR Chief Deputy as designee of the agency head.

As further detailed below, OSHR shall limit the issuance and use of State-issued mobile devices to the minimum required to carry out the agency's mission. In addition, State-issued mobile devices shall be used only for State business. As described below, there shall be a written justification for each State-issued mobile device that is issued. There shall also be a periodic audit of State-issued mobile device usage.

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

OSHR employees and authorized personnel, e.g., contractors, that have received authorization from OSHR's 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"). Mobile devices will be configured in accordance with the Statewide Information Security Policies and Mobile Policy Security Technical Implementation Guides (STIGS).

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 State data on their mobile device(s) that is essential to their role. This may include confidential personnel file information as defined by N.C.G.S. 126-22(b)(3), as working with personnel file data is inherent in the job duties for OSHR employees. When messages are sent to or from OSHR's legal counsel, this also will include confidential attorney-client communications or attorney work product. The access and download of other data classified as confidential per N.C.G.S. Chapter 132 is strictly prohibited, unless approved by OSHR's CIO or designee.
- State-issued mobile electronic devices shall be used only for State business.[1]
- Users must immediately report all lost or stolen devices using OSHR's incident response process and in accordance with the State's incident response process (See Statewide Incident Response

[1] Per the OSHR Acceptable Use Policy, which matches the DIT Statewide Acceptable Use Policy, "limited (incidental and occasional) personal use may be permissible when authorized by your management" and when the use meets the other requirements found in Section 3 of the policy.

Policy, IR-6 - Incident Reporting).

- If a user suspects that unauthorized access to State data has taken place via a mobile device, the user must report the incident using OSHR'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.

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 OSHR's 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 OSHR services that they are authorized to access. Individuals will need to use the Microsoft Outlook application to access State email on personal mobile devices.

All users should note that connection of a personal mobile device 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, for State-issued devices, with the OSHR Acceptable Use Policy (AUP)

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 locked 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.

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.
- Devices that are unassigned or re-assigned as part of offboarding/onboarding procedures.

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.

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.

PROCEDURES

REQUESTING AND RECEIVING DEVICES

1. Employee or supervisor requests mobile device based on business need as described in the Policy section of this document by sending an email to OSHR's CIO or designee with the following information:
    a. Employee name
    b. Supervisor name
    c. Division Director name
    d. Justification of how device will be used
    e. Desired device, if known

2. OSHR Division Directors will assess the need for an employee to have a mobile device, such as smartphones, MiFi devices and tablet computers. This will be sent to the OSHR Chief Deputy for approval. The Director of OSHR delegates this authority to the OSHR Chief Deputy.
    a. OSHR shall limit the issuance of mobile devices to the minimum required to carry out the agency's mission. OSHR will interpret this requirement as limiting the issuance of mobile devices to employees for whom access to a mobile electronic device is a critical requirement for job performance.

3. Upon the Chief Deputy's approval, OSHR's CIO or designee will complete the cellular provider's request template via email with specific device, accessories and plan selected along with associated one time and recurring cost.
    a. The device issued and the plan selected shall be the minimum required to support the employees' work requirements. This shall include considering the use of pagers in lieu of a more sophisticated device.
    b. The requirement for each mobile device issued shall be documented in a written justification that shall be maintained by OSHR's CIO or designee and reviewed annually.

4. Employee receives device and signs acknowledgment of receipt.

RETURNING DEVICES

1. Employee or supervisor returns device to OSHR CIO or designee to cancel service.
    a. Mobile numbers for senior leadership and select OSHR Division Director positions will be retained in a situation of personnel change and will be reassigned accordingly.

2. OSHR CIO or designee cancels service and either retains device for reuse or surpluses.
    a. Device will be wiped as part of offboarding/onboarding procedures in accordance with the Data Sanitization subsection as described in the Policy section of this document.

REPORTING REQUIRMENTS

OSHR Division Directors, in consultation with the Information Technology Services Division and the Office of State Budget and Management, shall document and review all authorized cell phone, smart phone, and other mobile electronic communications device procurement, and related phone, data, Internet, and other usage plans for and by their employees.

OSHR shall conduct quarterly audits of mobile device usage to ensure that OSHR employees and contractors are complying with mobile device policies and State requirements for their use.

- OSHR CIO or designee will be responsible for maintaining an up-to-date inventory of active mobile devices in a centralized system of record via Verizon Management Portal or a Mobile Device Management system.

OSHR shall report annually to the Chairs of the House of Representatives Committee on Appropriations and the House of Representatives Subcommittee on General Government, the Chairs of the Senate Committee on Appropriations and the Senate Appropriations Committee on General Government and Information Technology, the Joint Legislative Oversight Committee on Information Technology, the Fiscal Research Division, and the Office of State Budget and Management on the following:

- Any changes to agency policies on the use of mobile devices.
- The number and types of new devices issued since the last report.
- The total number of mobile devices issued by the agency.
- The total cost of mobile devices issued by the agency.
- The number of each type of mobile device issued, with the total cost for each type.

ACKNOWLEDGMENT

OSHR employees and contractors must acknowledge in writing that they have received a copy of this policy. Written acknowledgement is also required annually each fiscal year.

I have read, understand, and will abide by the above Mobile Device Policy when using a mobile device and other electronic resources owned, leased, or operated by the state. I further understand and will abide by the above Mobile Device Policy when using personal devices not owned, leased, or operated by the state. I further understand that I have no expectation of privacy when connecting any device to the State Network and that any violation of the regulations above is unethical and may constitute a criminal offense. Should I commit any violation of this policy, my access privileges may be revoked, disciplinary action may be taken, and/or appropriate legal action may be initiated.

_____ _____

Name *Date*

_____

User Signature

REFERENCES AND APPLICABLE LAWS

N.C.G.S. 143-162.5. Use of mobile electronic devices
N.C.G.S. Chapter 132 - NC Public Records Act
ITS Contract Number 915A