HR/LR Policy # 1438

Mobile Device Use

Date Issued: 12/7/2021
(Formerly part of HR/LR Policy #1423, Appropriate Use of Electronic Communication and Information Technology)

Date Revised: 07/01/2024

Authority: MMB Enterprise Employee Resources and Minnesota IT Services

OVERVIEW

Objective

Establish a minimum standard for appropriate use of all state mobile devices and personal mobile devices when conducting state business and/or accessing state data or networks. This policy also provides guidance to executive branch agencies on balancing the benefits of mobile device use with the requirements of legal compliance and data security.

Policy Statement

By using a state mobile device or a personal mobile device to conduct state business or to access state data, networks, or other IT resources (e.g., email, voice communication, data, text, messaging, etc.), employees acknowledge, understand, and agree to comply with this policy and all applicable statewide or agency policies. Employees who violate this policy may be subject to discipline, up to and including discharge.

Agencies may, at their sole discretion, deny or prohibit employees from using a state mobile device, or prohibit or limit an employee's use of a personal mobile device to conduct state business or to access state data, networks, or other IT resources.

Employees must protect the security, availability, and integrity of agency and state of Minnesota data stored, accessed, transmitted, or processed on a mobile device.

Scope

This policy applies to all employees of executive branch agencies (M.S. 43A.02, subds. 2 & 22) and includes all employees of the Minnesota State Retirement System, Public Employees Retirement Association, and Teachers Retirement Association.

Definitions and Key Terms

Key Term	Definition
Mobile Device	A portable and self-contained electronic device that can store, access, process, or transmit data, text, or email. This can include individual, shared, and test devices. Examples of mobile devices may include, but are not limited to, mobile phones, smartphones, laptops, tablets, and modems allowing laptops to connect to mobile data networks.
Personal Mobile Device	Any mobile device that is not provided by a state agency.
State Mobile Device	Any mobile device provided by a state agency.
Incidental Use	Personal use of state IT resources that is minimal in terms of duration and frequency. The use must not result in any additional costs to the state or loss of state time or resources for their intended business purpose.
Information Technology (IT) Resources	Software, hardware (e.g. computers, telephones, etc.), documentation, programs (e.g. email, voicemail, etc.), systems, networks, information, and devices owned, leased, or provided by the state.
Mobile Device Management (MDM)	Software and business processes that allow IT administrators to control, secure and enforce policies on mobile devices.
Security Measures	Configurations, settings, and communication techniques on a mobile device that control the security, integrity, and availability of the device's data.

Exclusions

N/A

Statutory References

M.S. 43A.38, subd. 4, Code of Ethics for Employees in the Executive Branch, Use of State Property
M.S. Chapter 13, Government Data Practices
M.S. 138.17, Government Records; Administration
M.S. 169.475, Use of Wireless Communications Device
5 U.S.C., sections 7321 – 7326, Hatch Act
18 U.S.C., section 119, Wire and Electronic Communications Interception
18 U.S.C. 2701-2711, Stored Wire and Electronic Communications and Transactional Records Access

GENERAL STANDARDS AND EXPECTATIONS

This policy should be read in conjunction with other applicable policies, including those from Minnesota Management and Budget (MMB) and Minnesota IT Services (MNIT).

The Minnesota Government Data Practices Act (the "Act") governs the collection, creation, storage, maintenance, dissemination, and access to government data. Government data is defined in the Act as all data collected, created, received, maintained, or disseminated by any government entity regardless of its physical form, storage media or conditions of use.

By using a state mobile device or a personal mobile device to conduct state business or to access state data, networks, or other IT resources (e.g., email, voice communication, data, text, messaging, etc.), employees acknowledge, understand, and agree to comply with this policy and all applicable statewide or agency policies. Employees who violate this policy may be subject to discipline, up to and including discharge.

I. Mobile Device Usage

a. **Business Need Requirement.** Agencies may provide an employee with a state mobile device or mobile service plan if the agency determines, in its sole discretion, that the use serves a legitimate business need. Additionally, employees may use a personal mobile device to conduct state business or access state data, networks, or other IT resources only if doing so serves a legitimate business need. To determine if there is a legitimate business need, one or more of the following criteria should be considered:
   i. A mobile device is essential for the employee to perform specific duties listed in their position description.
   ii. A large portion of the employee's job or other factors require the employee to work away from their assigned office or work space.
   iii. The employee does not have an assigned work space and needs to access state system technology to perform their job duties.
   iv. There is a job requirement for agency to contact the employee when they are away from their assigned office or work space or outside their normal work hours.

   Agencies must consider the following factors to determine whether to provide an employee with a state mobile device or mobile device service plan:
   i. Business need.
   ii. The mobile device satisfies state and agency security measures and conditions.
   iii. Other applicable criteria as determined by MNIT or the agency.

b. **Agency Discretion to Deny, Prohibit, or Limit Use of Mobile Devices.** Agencies may, at their sole discretion, deny, prohibit, limit, or discontinue employees use of a state mobile device or use of a personal mobile device to conduct state business or to access state data, networks, or other IT resources (e.g., email, voice communication, data, text, messaging, etc.). Although agencies may deny, prohibit, limit, or discontinue mobile device usage for any reason, some reasons may include:
   i. The employee works with sensitive or not public data.
   ii. The employee works in a high security area.
   iii. The agency or employee's work is subject to discovery, litigation, or compliance requirements.
   iv. The employee is non-exempt under the Fair Labor Standards Act (FLSA).
   v. The employee is in a temporary or probationary employment status.
   vi. Other applicable criteria as determined by MNIT or the agency.

c. No expectation of privacy. Employees do not have any right or expectation of privacy when using state mobile devices or when using personal mobile devices for state business and/or to access state data, networks, or other IT resources (e.g., email, voice communication, data, text messaging, etc.).

i. **State mobile device.**

1. The state maintains the right to monitor, read, examine, seize, or confiscate any state mobile device at any time, with or without cause or notice.
2. Agencies may override text message 'auto-delete' function on state mobile devices.
3. Employees are expected to maintain the security and privacy of all data classified as private, not public, or confidential under the Act or any other law.
4. Electronic monitoring of telephone conversations will only occur if proper notice has been given, in accordance with Federal regulations for Stored Wire and Electronic Communications and Transactional Records Access (Federal Wire Tap Regulations) 21 U.S.C. 2701-2711.
5. Refer to "Monitoring" in HR/LR Policy #1423 Appropriate Use of Electronic Communication and Information Technology.

ii. **Personal mobile device.**

1. The use of a personal mobile device for state business and/or to access state data or networks may result in the collection, creation, storage, or maintenance of government data, and this data is subject to the provisions of the Act and all other legal requirements.
2. Employees are expected to maintain the security and privacy of all data classified as private, not public, or confidential under the Act or any other law.
3. If the agency receives a request for data under the Act, or if the agency receives a request for data in discovery or in relation to other legal proceedings, the employee is responsible for providing to the agency all responsive data stored on any personal mobile device used for state business, and must cooperate with the agency's efforts to obtain such data from the mobile device, which may include providing the personal mobile device to the agency or to MNIT.
4. Employees are expected to cooperate with agency or MNIT requests to access personal mobile devices that are used to conduct state business and/or access state data or networks in order to:
   (a) Implement security controls.
   (b) Respond to discovery requests in administrative, civil, or criminal proceedings.
   (c) Audit compliance with state policies and procedures regarding the use of state data.
   (d) Conduct investigations into employee misconduct.
   (e) Other business purposes as determined by the agency or MNIT.
5. To the extent reasonably possible, the agency/MNIT will not retain or use any personal data stored or maintained on the personal mobile device.

d. Wage and Hour Issues

Non-exempt employees under the Fair Labor Standards Act must be compensated for agency work they conduct with their mobile devices, including if the work occurs outside of their normal working hours. The employee must keep track of the time worked and promptly report this time to their supervisor. Non-exempt employees must obtain supervisory pre-approval before working overtime hours.

e. Employee Safety

In accordance with the State of Minnesota Model Fleet Safety Management Standards employees must not talk on a mobile device while driving on work time unless there is a hands-free option. Employees **must follow all state laws regarding mobile devices and motor vehicle operation, including the hands-free law** and not, under any circumstances, compose, read, or send an electronic message when the vehicle is in motion or a part of traffic, in accordance with state law.

II. State Mobile Devices

Employees who are issued state mobile devices may use the device for state business purposes only, except as otherwise specifically provided in this policy and HR/LR Policy #1423 Appropriate Use of Electronic Communication and Information Technology.

a. Authorization

Agencies providing state mobile devices are expected to maintain and oversee compliance with this policy, MNIT Services standards, and all applicable state and federal laws. Agencies are responsible for:

i. Determining and documenting the business need for the state mobile device.
ii. Obtaining and retaining written acknowledgment from the employee acknowledging the applicable policies and procedures regarding their use of the state mobile device.
iii. Reviewing and documenting on an annual basis that there is a continued business need for the device.
iv. Ensuring related documentation is retained in accordance with applicable record retention schedules.

By using a state mobile device, employees agree to the following conditions:

i. The employee allows any required software to be loaded onto the device.
ii. The employee agrees and abides by the security measures and user authentication methods deemed necessary by MNIT Services and their agency.
iii. At their sole discretion, the employee's state agency or MNIT may remotely wipe all data (business and personal) from the device if required by business necessity.
iv. The device must be provided on demand for security audits; if there is data content related to a disciplinary or legal proceeding or a data request; or for any other business purpose.
v. Private or confidential government data must not be stored or downloaded onto the device except through secure portals established by MNIT Services.
vi. Device functionality may not be modified except as permitted by MNIT Services or the employee's agency.

State mobile devices are state property and employees must comply with all agency or MNIT requirements with respect to the state mobile device. When an employee is no longer authorized to use a state mobile device, or when the employee separates from their agency, the employee must turn in their state mobile device to their agency or to MNIT.

b. Government Data

Data collected, created, received, maintained, or disseminated from state mobile devices is considered government data and is subject to the Government Data Practices Act This information may include but is not limited to:

i. Call detail (e.g., time, number, date, duration) of calls appearing on the state mobile device billing account.
ii. Text messages and emails sent to or received from state-owned mobile devices.
iii. Any other files such as photos, voicemails, or attachments received or generated while performing state job duties.

f. Number Portability

Porting an employee's personal mobile phone number to a state billing account or a state mobile phone number to an employee's billing account is strictly prohibited. When employment ends the phone number on the state mobile device will not be released to the user for personal use.

g. Personal Use

Personal use of state mobile devices is allowed only for minimal, incidental use. Agencies reserve the right to seek reimbursement for personal use of any state mobile device.

h. Loss or Theft

If the state mobile device is lost or stolen, the employee must notify the MNIT Service Desk as soon as possible but no later than the next business day.

III. Personal Mobile Devices

Agencies cannot require an employee to conduct state business specifically on a personal mobile device. However, if an employee is required to perform work away from their assigned office or work space, or outside their normal work hours, the agency can require the employee to be available to perform work via a method provided by the employee (e.g., personal mobile device, land line, Internet voice). The use of a personal mobile device for multi-factor authentication using an agency-approved authentication application does not create or store any data on the personal device. As such, there is no data that could be retrieved from the personal device for data collection.

a. Authorization

By using a personal mobile device to conduct state business or access state data or networks, employees agree to the following conditions:

i. The agency and MNIT have the authority to monitor use in conducting state business or accessing state data or networks.
ii. For the state's Mobile Device Management (MDM) or other required security software to be loaded onto their device.
iii. To abide by the security measures and user authentication methods deemed necessary by MNIT Services and their state agency.
iv. The agency or MNIT may, at their sole discretion, wipe all government data and remove access to applications on the device if required by business necessity. During this process, attempts will be made to safeguard personal data and applications, but it cannot be guaranteed.
v. The device must be provided on demand for security audits; if there is data content related to a disciplinary or legal proceeding; or for any other business purpose.
vi. Private or confidential government data must not be stored or downloaded onto the device except through secure portals established by MNIT Services.

Employee must allow their agency or MNIT Services to remove and disable any state provided third-party software, services, and government data from the device, or delete such items at the agency's or MNIT's direction. Employees must allow this when they no longer use their personal mobile device for state business or to access state data or networks, including when they are no longer authorized to use it for state business, when they separate from their agency, or if they choose to no longer use it.

b. **Government Data.** By using personal mobile devices to conduct state business, whether or not the personal mobile device accesses the state's data or networks, employees may intentionally or inadvertently create electronic records on those devices relating to their work. These records may include:

i. Text messages
ii. Voicemails
iii. Emails
iv. Other electronic communications or files

In accordance with the Minnesota Government Data Practices Act, Minn. Stat. chapter 13, these work-related records are defined as government data. Employees are expected to manage government data consistent with the Act and in accordance with any applicable retention or security policies. Government data should not be stored solely on a personal mobile device but should also be saved on a state system network drive.

c. Data Requests. When needed to respond to requests under the Government Data Practices Act or in relation to legal proceedings, the employee must provide access to all requested government data that is on a

personal mobile device. This may require the agency or MNIT to copy the entire device, including personal information, because it may not be able to differentiate or otherwise separate personal and government data.

d. Loss or Theft. When a personal mobile device that contains government data or accesses state data or networks is lost or stolen, the employee must take steps to protect the security and privacy of the data and networks and comply with applicable security incident requirements. The employee must:

i. Report the incident to the MNIT Service Desk as soon as possible but no later than the next business day.

ii. Provide evidence that the device has been remotely wiped or made inoperative to assure the security of the government data and state networks that may be present on or accessible through the device.

iii. Make available to the agency any business information stored within any backups of the personal mobile device.

e. Replacement. If the employee whose personal mobile device contains government data or accesses state data or networks gets a new device or replaces their personal mobile device the employee must:

i. Remove all state applications and data from the personal mobile device being replaced.

ii. Notify the MNIT Service Desk that the device had been replaced as soon as possible but no later than the next business day.

f. **Allowances / Reimbursements.** Allowances / reimbursements for personal mobile devices used for state business are only permitted as provided in the applicable collective bargaining agreement (CBA) or compensation plan. No reimbursements or allowances are permitted for employees whose CBA or compensation plan does not provide for personal mobile device reimbursements or allowances. Refer to the employee's CBA or compensation plan to determine the availability, amount and terms of any personal mobile device allowances or reimbursements.

RESPONSIBILITIES

Agency Responsibilities

- Adopt and comply with the provisions of this policy.
- Authorize the use of state or personal mobile devices based on business necessity.
- Provide awareness of this policy and MNIT Services' standards to employees.
- Maintain an escalation process to ensure lost or stolen devices are addressed promptly.
- Develop supplemental addenda as needed, to address agency specific needs that are consistent with this policy and the law.
- Procure state devices based on business necessity and manage applicable state contracts.
- Safeguard and maintain state devices and applicable software to state security standards.
- Review monthly mobile device billings, just as any other type of billing the agency receives. Agencies may use their discretion in determining who performs this review.
- Conduct at least an annual review of the individual state mobile device assignments to determine if there is a continuing business need that remains cost justified.
- Collect state mobile devices when the employee separates from the agency or the business need for the state mobile device ceases.
- Ensure separating employees provide to the agency (or delete if permitted by the records retention policy) all government data stored on a personal mobile device, and ensure all applications on personal mobile devices that allowed access to state data or networks are deleted or disabled.
- Notify MNIT when employees who used personal mobile devices to access state data or networks separate from the agency so that MNIT Services can remove or disable any state provided third-party software and services.

MMB Responsibilities

- Administer and maintain this policy in conjunction with MNIT Services.
- Consider agency policy exception requests in conjunction with MNIT Services (e.g. special agents undercover).

MNIT Responsibilities

- Maintain the technology and security related policies and standards as it relates to mobile devices.

Employee Responsibilities

- Comply with all provisions of this policy.
- Protect the state mobile devices and personal mobile devices that contain government data or access state data or networks from theft, damage, abuse, and unauthorized use.
- Comply with MNIT Services' security measures and standards.
- Comply with agency-specific policies and procedures.

FORMS AND INSTRUCTIONS

The Acknowledgement Form for HR/LR Policy #1438 Mobile Device Use is included in annual ELM training for all state agency employees.

REFERENCES

HR/LR Policies

1423, Appropriate Use of Electronic Communication and Information Technology
1445, Code of Ethical Conduct

Enterprise Information Security Policies & Standards

CONTACTS

MMB Human Resource Management and MMB Labor Relations