NIH Policy Manual

0002 - NIH Mobile Device Policy

Issuing Office: OD/OCIO **Phone:** (301) 496-1168

Issuing Office Email: nihciocommunications@mail.nih.gov

Issuing Office Website: https://ocio.nih.gov/

Release Date: 5/18/2021 ? **Technical Revision Date:** 1/12/2023 ?

Transmittal Notice

1. **Explanation of Material Transmitted:** This policy establishes requirements for the management and use of mobile devices at the NIH. This revision extends the temporary policy and updates requirements in Section C. Policy regarding accountable property and lines of service/rate plans.
2. **Filing Instructions:**

    - **Insert:** NIH Policy Manual, Chapter 0002, dated 5/18/2021
    - **Expiration:** This temporary policy expires within 2 years of publication, afterwards the OCIO will issue a standing policy within the 2800 series.

1. **PLEASE NOTE:** For information on:

    - Content of this chapter, contact the issuing office listed above.
    - NIH Policy Manual, contact the Division of Compliance Management, OMA on 301-496-4606, or enter this URL: https://oma.od.nih.gov/DMS/Pages/Manual-Chapters.aspx.

A. Purpose

This policy establishes the minimum requirements for the management and use of mobile devices at the NIH.

NIH Institutes and Centers (ICs) shall implement this policy or may create more stringent policies and procedures, but none less restrictive.

B. Scope

This policy applies to "NIH mobile devices" (i.e., cell phones, smart phones, tablets), approved for use by the NIH, that wirelessly or physically connect to internal NIH information technology (IT) resources, including the NIH network (NIHnet) or synchronizing

with the NIH enterprise services such as email, cloud-hosted file storage and collaboration sites. It does not apply to laptops.

There are two classes of NIH mobile devices: Government Furnished Equipment (GFE) that are acquired and managed by NIH; and Non-Government Furnished Equipment (Non-GFE), including personally owned devices and devices provisioned by other entities, such as a contractor or as part of a research contract.

This policy does not apply to mobile devices that only connect to the NIH **guest** network and do not store, process or transmit NIH information.

This policy does not supersede any other applicable law or higher-level agency directive.

C. Policy

1. NIH mobile devices may only access NIH IT resources through the approved enterprise-wide Mobile Device Management (MDM) service.

    a. Government furnished mobile devices must be enrolled in this MDM service before being allowed direct access to NIH IT resources.
    b. Mobile devices that are personally owned or contractor-furnished mobile devices may only access NIH IT resources through an application "container" managed by the approved, enterprise-wide MDM service.

2. Acceptance of the appropriate NIH Rules of Behavior and End User Agreement will be required for users with mobile devices enrolled in the NIH enterprise MDM service and connecting to NIH IT resources (see appendices 1 and 2). Accepted user agreements will be maintained by: 1) the users' respective IC in accordance with applicable IC procedures and NIH records schedules; or 2) the *NIH Information Security and Privacy Awareness* training system.
3. Mobile devices used for official business must not be modified to circumvent the manufacturer's operating system security features (e.g., "jailbreaking" or "rooting") or attempt to circumvent the NIH configurations and security controls implemented as part of the MDM service.
4. Each IC will designate and maintain one or more Mobile points of contact (POC) to ensure their IC manages all government furnished mobile devices consistent with this policy and any applicable IC policies and procedures.
5. All mobile devices—both government furnished and non-government furnished—must comply with the NIH MDM technical specifications.
6. All mobile devices must be password-protected. Enhanced authentication may be used for devices that have the functionality (e.g., biometrics).
7. All mobile devices must implement a time-out function that requires a user to re-authenticate after inactivity.
8. Lost or stolen mobile devices—both government furnished and non-government furnished—must be reported to the NIH IT Service Desk within one hour (60 minutes) so that the government information on the device can be remotely removed.

9. Lost or stolen government furnished mobile devices must be reported to the IC property custodian so that a Report of Survey can be conducted.
10. ICs must ensure their offboarding processes for Federal staff and contractors include measures to ensure that government furnished devices are returned to their respective IC Mobile POC before separation, and that non-government furnished devices have the NIH MDM container removed within 24 hours of separation.
11. More than one line of service/telecommunications account on a given device through the addition of SIM cards or other means are prohibited on government furnished mobile devices.
12. Purchases of wireless telecommunications rate plans (except those devices used in scientific research) must conform with the NIH-negotiated rates with the wireless carriers. Contact your IC Mobile POC to access those rate plans.
13. Government furnished mobile devices are not accountable property, except for tablets. Tablets (with or without wireless capability) must be maintained as accountable property in the NIH property management system.
14. All government furnished mobile devices that include phone capabilities shall have the phone number maintained in the NIH Enterprise Directory for emergency alert (Alert NIH) notifications.

D. Roles and Responsibilities

The primary individuals listed below may assign a designee, as appropriate, to carry out these responsibilities:

1. NIH Chief Information Officer (NIH CIO)

   The NIH CIO establishes and ensures the implementation of this policy at NIH consistent with all other Federal, HHS, and NIH rules and regulations.

1. IC Executive Officers (IC EO)

   The IC EO is responsible for designating one or more IC Mobile point(s) of contact (POC) and ensuring any IC policies are consistent with (or more restrictive) this policy.

1. IC Mobile Points of Contact (POC)

   The IC Mobile POC(s) is responsible for ensuring overall management of mobile devices consistent with the requirement of this policy and any IC related policies and procedures, including ensuring the accuracy of inventory information, adequacy of off-boarding procedures, and collection and maintenance of the IC's NIH Rules of Behavior and End User Agreement documentation.

1. Management Officials

   Management officials, in their supervisory role, are responsible for informing users (employees, contractors, interns, etc.) of their rights and responsibilities, including the dissemination of the information in this policy.

1. NIH Mobile Device User

   All NIH staff that use mobile devices to access NIH IT resources are responsible for ensuring compliance with this policy, and for reading, agreeing, and adhering to the applicable NIH Rules of Behavior and End User Agreement (See appendices 1 and 2).

E. Compliance

All mobile devices must comply with this policy.

Where deviations from this policy are necessary, requests for exceptions should be submitted to nihciocommunications@nih.gov, and will be evaluated by the NIH Chief Information Officer (CIO). A waiver request must include a business case for the exception that specifies how enforcement of this policy would restrict the mission of NIH and the compensating controls that will be implemented.

F. References

1. *HHS Policy for Mobile Devices and Removable Media*, available at: https://intranet.hhs.gov/working-at-hhs/cybersecurity/ocio-policies
2. HHS Memorandum - *Use of Government Furnished Equipment (GFE) During Foreign Travel*, available at: https://intranet.hhs.gov/working-at-hhs/cybersecurity/policies-standards-memoranda-guides/memoranda
3. *NIH IT General Rules of Behavior*, available at: https://ocio.nih.gov/InfoSecurity/Policy/Pages/Default.aspx
4. *NIH Procedure for Reporting Lost or Stolen Equipment*, available at: https://myitsm.nih.gov/nav_to.do?uri=%2Fkb_view_customer.do%3Fsys_kb_id%3D36f553edd1b1890062e3f01615533b2a
5. NIH Policy Manual, Chapter 1743 *Managing Federal Records*, available at: https://policymanual.nih.gov/1743/
6. *NIH Information Security Policy Handbook*, available at: https://ocio.nih.gov/InfoSecurity/Policy/Pages/default.aspx

   a. NIH Media Sanitization and Disposal Guidelines
   b. NIST Special Publication 800-88, Guidelines for Media Sanitization, available at: https://www.nist.gov/publications/nist-special-publication-800-88-revision-1-guidelines-media-sanitization

G. Definitions

Jailbreaking – In the mobile technology context, the term "jailbreaking" has colloquially meant removing limitations on devices running the Apple iOS operating system, permitting root access to the operating system, and allowing the download of additional applications and themes that may or may not be authorized by the manufacturer. The term has also sometimes

been applied to the process of gaining root access to non-Apple devices, known as "rooting."

Mobile Device – Small footprint computing devices that can be easily transported, such as cell phones, smart phones, and tablet computers (not laptops), approved for use by the NIH to wirelessly or physically connect to internal NIH information technology (IT) resources.

NIH Staff – Employees, contractors, students, guest researchers, visitors, and others who have access to NIH IT resources through the NIH Active Directory account structure.

NIH Information Technology (IT) resources – Any information technology systems, services, and data that is accessed via the NIH network (NIHnet), including use and synchronizing with NIH enterprise services such as email and cloud-hosted file storage and collaboration sites.

Government Furnished Equipment (GFE) – Devices and equipment that are purchased and funded by the NIH for use by NIH staff

MDM container – An application used to separate and secure NIH data and resources from the rest of the device. The container prevents malware, intruders, system resources or other applications from interacting with the application and data protected by the container. The container provides the ability to erase NIH specific data and components without affecting the rest of the device.

Non-Government Furnished Equipment (Non-GFE) - personally owned devices and devices that are provided by other entities, such as a contractor or as part of a research contract.

Sensitive information – At NIH, sensitive information is "information that has a degree of confidentiality such that its loss, misuse, unauthorized access, or modification could compromise the element of confidentiality and thereby adversely affect national health interests, the conduct of NIH programs, or the privacy of individuals entitled under the Privacy Act or the Health Insurance Portability and Accountability Act (HIPAA)." IT security personnel and system owners can equate this definition of sensitive information with data that has a FIPS 199 security impact level of Moderate or High for the confidentiality security objective. This definition of sensitive information is media neutral, applying to information as it appears in either electronic or hardcopy format. Examples of sensitive information include, but are not limited to, Personally Identifiable Information (PII) and Protected Health Information (PHI).

Appendix 1: NIH Rules of Behavior and End User Agreement for Government Furnished Mobile Devices

These rules hold NIH staff accountable for their actions when government furnished mobile devices are used to connect or synchronize with NIHnet and other NIH IT resources, either wirelessly or physically, including enterprise services such as email and cloud-hosted file storage and collaboration sites. Access and continued use of network services are granted on the condition that each user reads, acknowledges, and follows the NIH policies concerning the

use of mobile devices and services.

In accordance with NIH policies and procedures, I will:

- Ensure that the device is supported by the original operating system, receives current updates and security patches, and is registered with NIH Mobile Device Management (MDM) service prior to synchronizing or connecting to NIH IT resources.
- Use an acceptable passcode or PIN to access the government furnished device.
- Ensure NIH data is protected to the maximum extent practicable.
- Ensure the device is returned to my IC to be reused or disposed of properly in accordance with the NIH Media Sanitization and Disposal Policy.
- Notify the NIH IT Service Desk within one hour if the device is lost or stolen.

I Will Not:

- Download, store, or transfer sensitive information or data to the device. This excludes government email that is protected through the MDM service.
- Use my mobile device as the sole data repository for NIH information or data.

Acknowledgement Statement:

I have read the NIH Mobile Device Policy and Rules of Behavior, and I acknowledge, understand and will comply with the requirements.

- I understand that NIH has the right to restrict or rescind these privileges or take other administrative or legal action should I violate these rules or any other policies that govern mobile device usage at NIH.

Name: _____

Signature: _____ Date: _____

Appendix 2: NIH Rules of Behavior and End User Agreement for Non-Government Furnished Mobile Device

NIH offers staff the option of using non-government furnished equipment, such as their personally owned or contractor furnished mobile devices, for business use at NIH. These rules hold users of non-government furnished mobile devices with access to NIH network resources accountable for their actions. Access and continued use of NIH services is granted on condition that each user reads, acknowledges, and follows the NIH policies concerning the use of these devices and services.

In Accordance with NIH policies and procedures, I will:

- Ensure the device is registered with the NIH Mobile Device Management (MDM) service prior to synchronizing or connecting to NIH IT resources.

- Send and receive NIH email, store, and access data only through the NIH MDM container.
- Maintain the original device operating system and keep the device current with security patches and updates, as released by the manufacturer.
- Immediately delete any sensitive material that is downloaded onto the device.
- Notify the NIH IT Service Desk within one hour after if the device is lost or stolen.
- Notify appropriate IC personnel in the event I have a change of employment in which I would no longer require or need access to IC-specific or NIH information, and ensure the MDM container application(s) and any NIH data are removed from my device in a timely manner.

I will not:

- Download, store, or transfer sensitive information or data to the device. This excludes government email that is protected through the MDM service.
- Use my mobile device as the sole data repository for NIH information or data.
- Modify the device to circumvent the manufacturer's operating system security features.

Expectation of Privacy:

NIH will respect the privacy of the non-government furnished mobile device and its owner, and will only access the MDM container for routine maintenance activities and to implement security controls for forensic investigations or to respond to legitimate discovery requests.

The NIH will not use the MDM for the following:

- Location Tracking.
- Access to personal applications and data.
- Accessing and/or updating non-MDM device settings and configurations.
- Viewing and/or disseminating website search history and cookies on the device.

While NIH access to the device itself is restricted to the application container, NIH policies and rules of behavior regarding the use of information technology and access of government email and other government systems by the user of the device remain in effect.

Acknowledgement Statement & Agreement:

I have read the NIH Mobile Device Policy and Rules of Behavior, and I acknowledge, understand and will comply with the requirements as applicable to my non-government furnished device usage to access NIH IT resources.

- I understand that NIH has the right to restrict or rescind these privileges, or take other administrative or legal action should I violate these rules or any other policies that govern mobile device usage at NIH, including removal of the MDM container.
- I understand that addition of the MDM container application(s) may decrease the available memory or storage on my device and that NIH is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of the MDM service.
- I understand that contacting vendors for trouble-shooting and support of third-party software is my responsibility, with limited configuration support and advice provided by the NIH IT Service Desk.
- I understand that business use may result in increases to my monthly service plan costs. I further understand that government reimbursement of any business-related data or voice plan usage of my device is not provided. Should I later decide to discontinue my participation in the MDM service, I will notify the appropriate officials to remove and disable any MDM container application(s) and data from my device.

Name: _____

Signature: _____ Date: _____