

CHAPTER 11: Managing Mobile IT Devices Policy and Procedure

11-1 INTRODUCTION

In this new era of mobile computing, powerful hand-held devices, wireless communications, cloud services, and social networks are creating new boundaries that blur the lines between personal computing and corporate resources. Federal government agencies must embrace this new world and be ready to mobilize their business, transform their organizations, and modernize their technical infrastructures to meet the significant opportunities as well as challenges that mobility brings to the federal work place, including compliance with all applicable Federal laws and regulations.

Responding to today's mobile opportunities requires that we not only embrace and support the use of these new devices and technologies, but also manage and secure them. Mobile device management (MDM) tools provide the capabilities to secure, monitor, manage, and support mobile devices. MDM functionality typically includes inventory management, monitoring, administration, over-the-air distribution of applications, and data and configuration settings for all types of mobile devices, including mobile phones which are connected to the HUD network, smart phones, tablet computers, laptops, mobile printers, mobile POS devices, etc., for both government furnished and non-government furnished equipment. This policy does NOT apply to cellular phones, satellite phones, or any other device which does not connect to the HUD network. For more information about the policies regarding those telecommunication services and devices, see Department Handbook:

- Chapter 14 of Administrative Services Policy Handbook (2200.1); and
- Telecommunications Management (2241.1).

By controlling and protecting the data and configuration settings for all mobile devices in the network, MDM can reduce support costs and business risks. The intent of MDM is to optimize the functionality and security of mobile devices in our workforce while minimizing cost and downtime. Mobile IT devices increase the productivity of the Department's managers and employees by providing wireless communications to access HUD information systems when and where such access is needed. These devices can be used for a range of functions, including but not limited to telephone, electronic mail, address book, calendaring, and internet access. While these devices provide benefits to HUD employees and the organization, they also pose risks to the Department because they are easy to misplace or have stolen and are vulnerable to malware, spam, electronic eavesdropping, and other security threats that may result in exposure of sensitive information.

11-2 PURPOSE

The purpose of this policy is to establish an authorized method for controlling mobile computing and storage devices that contain or access HUD information resources. This policy is intended to manage the risks of mobile computing by providing guidelines ensuring that:

- HUD mobile computing assets are appropriately procured, managed, and secured, including compliance with all applicable Federal laws and regulations;

- The confidentiality, availability, and integrity of HUD information while at rest or in transit is protected; and
- Mobile users are properly trained and made aware of their responsibilities.

This policy applies to mobile IT devices bought by HUD (HUD-owned mobile IT devices) and those that are purchased by the individual (Bring Your Own Device (BYOD) program participants) and connected to the HUD network. This policy applies to smartphones and tablet devices¹.

These policies ensure that the mobile IT devices (HUD-owned or BYOD):

- Are used in a manner that is consistent with HUD's mission and achieve intended results;
- Are protected from waste, fraud, and mismanagement; and
- Adhere to applicable laws, regulations, and guidelines.

11-3 AUTHORITIES

This policy ensures compliance with the following statutes, directives, and guidance:

- E-Government Act of 2002 (44 U.S.C. Ch 36);
- Privacy Act of 1974 (5 U.S.C. 552a);
- Federal Information Security Management Act of 2002 (FISMA), [Title III of the E-Government Act of 2002 (44 U.S.C. Ch 36)];
- Clinger-Cohen Act of 1996 (40 U.S.C 11315);
- Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources;
- OMB Circular A-123, Management Accountability and Control;
- National Institute of Standards and Technology (NIST) Special Publication 800-124, Guidelines for Managing and Securing Mobile Devices in the Enterprise;
- NIST Special Publication 800-121, Guide to Bluetooth Security;
- NIST Special Publication 800-48, Wireless Networks Security: 802.11, Bluetooth and Handheld Devices;
- NIST Special Publication 800-46, Guide to Enterprise Telework and Remote Access Security;
- NIST Special Publication 800-45, Guidelines on Electronic Mail Security;
- NIST Special Publication 800-53, Recommended Security Controls for Federal Information Systems and Organizations;
- National Telecommunications and Information Administration Manual of Regulations & Procedures for Federal Radio Frequency Management (January 2000 Edition with January/May/September 2001 versions);
- 47 Code for Regulations, Telecommunications Parts 0-199;

¹ A complete list of HUD-approved mobile IT devices and operating systems can be obtained on the site: <http://hudatwork.hud.gov/po/i/2010/automation.cfm>.

- Office of Management and Budget Circular A-130, Efficient Management of Federal Information Resources;
- NIST Guidelines on Cell Phone and PDA Security, 2008;
- National Archives and Records Administration, Encrypt all data on mobile computers/devices, 2009;
- Executive Order Promoting Efficient Spending, 2011;
- Executive Order Federal Leadership on Reducing Text Messaging While Driving, 2009;
- Freedom of Information Act (5 U.S.C. 552);
- Federal CIO Council's "A Toolkit to Support Federal Agencies Implementing Bring Your Own Device (BYOD) Programs", 2012; and
- Employee limited usage, in Chapter 8 and Appendix 6 of HUD Handbook 2400.1, REV-1, CHG 2, regarding "Limited Personal Use" of Government Office Equipment Policy".

11-4 POLICY

It is the policy of HUD to develop and maintain security control standards for all HUD-owned mobile IT devices that create, access, process or store HUD information, and the information created, collected, and processed on behalf of HUD on these devices. This policy also covers personally-owned mobile IT devices that access or store HUD information. These standards are part of the overall HUD Mobile Information Technology Devices Program authorized by the HUD Mobile IT Devices Policy and Procedures and must be followed by all personnel with either a HUD- owned mobile IT device or a device that participates in the BYOD program. The Office of the Chief Information Officer (OCIO) directs and oversees compliance with the security control standards for mobile IT devices. Therefore, the following policy is established to adequately safeguard the management of mobile IT devices connected to HUD's network. Mobile device care is the responsibility of each mobile device user. Failure to adhere to the guidelines listed below may result in personal liability and/or retraction of device privileges.

- A. This policy applies to all departmental employees and to all departmental offices and organizations, including headquarters, regional, and field locations.
- B. Only HUD OCIO-authorized mobile IT devices may be connected to the HUD network.
- C. Use of email should be in conformance with HUD policies herein and in Chapter 8 and Appendix 6 of HUD Handbook 2400.1, REV-1, CHG 2, regarding "Limited Personal Use" of Government Office Equipment Policy".
- D. It is prohibited to distribute HUD-owned mobile IT devices to contract personnel, Fair Labor Standards Act (FLSA) covered employees, interns, or other non-government employees. Requests for a FLSA-covered employee waiver to this policy must be approved by the General Deputy Assistant Secretary (GDAS) or designee.
- E. Authorized use of mobile IT devices includes any activities that:
 1. Directly support official Government business activities and communications, and

2. Are in accordance with the following:

- Information Technology Security Policy, HUD Handbook 2400.25, Rev. 1 (to be referred to as the IT Security Handbook)
 - Information Resource Management Policy, HUD Handbook 2400.1
 - Limited Personal Use of Government Office Equipment Policy, HUD Handbook 2400.1, Chapter 8
 - HUD Departmental Rules of Behavior² and Rules of Behavior for Connecting Mobile IT Personal Device to HUD Resources as applicable.
- F. Use of HUD-owned IT devices for other than authorized Government business or limited personal use is prohibited. Use of BYOD devices while connected to HUD resources via the Mobiles Device Management solution are limited only to authorized Government business within the secure solution. Personal use of BYOD devices are not restricted outside of the secure Mobile Device Management solution.
- G. All mobile IT devices (HUD-owned and BYOD) which are configured for HUD resource connectivity that are lost or stolen will have the HUD resources remotely wiped and HUD electronic mail redirected. The U.S. Computer Emergency Readiness Team (US-CERT) will also be notified of this incident by the OCIO.
- H. Access to HUDMobile from a mobile IT device is not supported by OCIO.
- I. Classified information is not authorized on any mobile IT device. Information stored on the device (either HUD owned or BYOD) is subject to the requirements of the Freedom of Information Act and is considered discoverable.
- J. It is illegal to obtain, attempt to obtain, or assist another in obtaining departmental mobile IT devices through activities that involve waste, fraud, abuse, or mismanagement.
- K. Misuse of departmental resources via a mobile IT device may result in administrative and disciplinary actions. For more details, see the Enterprise Rules of Behavior for HUD Employees and Contractors.
- L. This policy does not supersede or imply authorized use of mobile IT devices outside official duty hours.

² The U.S. Department of Housing and Urban Development Departmental Rules of Behavior can be found at <http://portal.hud.gov/hudportal/documents/huddoc?id=rulesofbehavior.pdf>.

11-5 ROLES AND RESPONSIBILITIES:

Management of mobile IT devices (both HUD-owned and those used by BYOD program participants) is led by the OCIO. It is the OCIO's responsibility for managing these devices to ensure that the mobile IT devices connected to HUD resources are configured in accordance with all applicable federal and departmental policy and procedures. As part of this duty, the OCIO has established this policy and associated guidance for the management of all mobile IT devices connecting to HUD resources. The following section details the roles and responsibilities for each method of connecting to HUD resources.

A. HUD-owned Mobile IT Device

Government employees do not have a right, nor should they have an expectation, of privacy while using HUD-owned mobile IT device at anytime, including accessing the Internet and using e-mail and voice communications. To the extent that employees wish that their private activities remain private, they should avoid using the HUD-owned mobile IT device for limited personal use. By acceptance of the HUD-owned mobile IT device, employees imply their consent to disclosing and/or monitoring of device usage, including the contents of any files or information maintained or passed -through that device.

A1. Office of the Chief Information Officer will:

1. Centrally negotiate, acquire, support and manage the delivery of HUD-owned mobile IT devices and associated services and licenses to realize cost efficiencies, ensure accountability and control of Departmental resources, and ensure compliance with federal technology and security standards.
2. Work with the Program and Support Office annually to adequately plan for HUD-owned mobile IT device requirements during each budgetary cycle, as required by HUD's established IT Capital Planning process.
3. Identify the baseline number of HUD-owned mobile IT devices to be funded, maintained, and supported by the OCIO and allocated to the Office of the Secretary, Senior Executive Service (SES), and the Program and Support Offices. Additional HUD-owned mobile IT device requirements will be assessed annually by the OCIO, with input from the Program or Support Offices, through the IT Capital and Acquisition planning processes. This process will also be used to update the mobile IT device baseline. If the Program or Support Office determine that additional HUD-owned mobile IT devices are required beyond the baseline, the Program and Support Offices will be required to provide funding for the purchase and maintenance of the additional devices and services. OCIO will provide information to the Program and Support Offices regarding mobile IT device industry information (i.e., current features, services, and associated costs) and management information (i.e., inventory listing and usage) to ensure effective and prudent use.

4. Distribute and manage the HUD-owned mobile IT devices for the Department, in accordance with established IT Capital Planning and IT acquisition requirements.
5. Provide funding and support resources, as approved by the IT Capital Planning process, for HUD-owned mobile IT devices for the Office of the Secretary, Senior Executive Service (SES), and approved personnel. The Program and Support Offices will be required to provide funding for the purchase and maintenance of HUD-owned mobile IT devices and services that are beyond the number of devices funded by OCIO. OCIO will provide information to the Program and Support Offices regarding HUD-owned mobile IT device features, services, and associated costs to ensure effective and prudent use.
6. Ensure that HUD-owned mobile IT devices comply with applicable IT security policies and guidance. HUD will use a Mobile Device Management (MDM) solution to manage and monitor mobile devices issued to HUD employees. The MDM will enforce mobile security settings that include:
 - a. Requiring a password to access each mobile IT device. Failure to enter the password successfully after 10 attempts will result resetting the device to factory default setting and in the automatic wiping of the device.
 - b. Requiring the use of a complex password that includes a minimum of one (1) alpha, one (1) numeric, and one (1) special character.
7. Monitor and review HUD-owned mobile IT device activities to ensure:
 - a. A sound understanding of HUD-owned mobile IT device needs in support of continuous and effective Departmental communications;
 - b. A proper balance between HUD-owned mobile IT device cost and customer satisfaction requirements;
 - c. Compliance with regulatory requirements and standards for HUD-owned mobile IT devices;
 - d. Realization of cost savings and/or cost avoidance in the acquisition and management of mobile IT devices; and
 - e. The optimal benefits are realized from investments in HUD-owned mobile IT devices and services in supporting program delivery.
8. Provide advice and assistance to Program and Support Offices regarding HUD-owned mobile IT devices to ensure effective and prudent use.
9. Periodically conduct surveys to ensure that HUD-owned mobile IT devices and services are being acquired at the most economical costs available.
10. Provide leadership, guidance, and oversight in the establishment and maintenance of inventories of HUD-owned mobile IT devices, and associated software and licenses, where applicable.
11. Ensure that HUD-owned mobile IT devices and services are upgraded as required to provide reliable voice and data capabilities.
12. Monitor and manage the level of availability, performance, and restoration for HUD-owned mobile IT devices and associated services.

13. Notify the appropriate Program or Support Office of receipt of any damaged or returned HUD-owned mobile IT devices.
14. Develop and disseminate annual HUD-owned mobile IT device reports for each Program and Support office.
15. Develop and disseminate quarterly usage reports to ensure adequate and appropriate HUD-owned mobile IT device usage. OCIO reserves the right to terminate government-provided services for the HUD-owned mobile IT device for non-use. The policy for terminating voice and data services for non-use is 30 days.
16. Conduct annual user update requests for HUD-owned mobile IT devices.
17. Ensure that Program and Support offices comply with the provisions of the HUD-owned mobile IT device guidance.
18. Establish and maintain security configurations for all HUD-owned mobile IT devices, including patching and upgrading of software/firmware.
19. Develop and maintain applicable Mobile Device policies, procedures and guidelines regarding HUD-owned IT mobile device management. OCIO reserves the right to recall/disconnect government-provided mobile devices due to budget restrictions or changes to deployment priorities.
20. Provide basic device training to users who are issued a HUD-owned mobile device.

A2. Program and Support Offices will:

1. Establish the General Deputy Assistant Secretary (GDAS) or designee for each Program and Support Office who will serve as the authorized individual for approving and submitting requests to the OCIO for HUD-owned mobile IT devices and services.
2. Submit approved requests for HUD-owned mobile IT devices and services to the OCIO, and confirm funding availability through the GDAS.
3. Identify business and program requirements and work with the OCIO to develop standardized, cost-effective solutions based on a common telecommunications infrastructure.
4. Review the OCIO HUD-owned mobile IT device usage reports to ensure that the office is using these devices adequately and effectively; and take the necessary actions to eliminate redundant, unauthorized, or unused HUD-owned mobile IT devices.
5. Maintain inventories of the office's HUD-owned mobile IT devices and ensure compliance with associated monitoring requirements from the OCIO.

6. Include, as necessary, HUD-owned mobile IT device requirements as part of the IT Capital Planning process.
7. Submit approved waiver requests to the OCIO for distribution of HUD-owned mobile IT devices to Fair Labor Standards Act (FLSA) covered employees, interns, or other non-government employees.
8. Notify OCIO of any separation, transfer, or termination from the Department of any personnel using HUD-owned mobile IT devices so that OCIO can take the appropriate actions.
9. Notify OCIO of any employee that is approved to use a HUD-owned mobile device during official international travel. International roaming services may be available on a temporary basis for business travel only. Data rate plans for e-mail and broadband cards are an additional cost to HUD for mobile device users traveling outside the Continental U.S.
10. Confirm individuals with a HUD-owned mobile IT device with the OCIO on an annual basis.
11. Ensure that the office and applicable employees comply with the provisions of the HUD-owned mobile IT device guidance.

A3. Employees will:

1. Complete the IT Security Awareness Training within the designated timeframe and understand the security risks associated with use of mobile IT devices prior to requesting service or equipment.
2. Request HUD-owned mobile IT devices through the authorized individual in their office.
3. Comply with HUD Rules of Behavior and comply with departmental Limited Personal Use of Government Office Equipment policy.
4. Use a complex password that includes a minimum of one (1) alpha, one (1) numeric, and one (1) special character. This password is required to access the device and failure to successfully enter the password after 10 attempts will result in the device resetting to factory defaults and automatically wiping the device.
5. Any applications required for HUD work need to be submitted to the HUD National Help Desk in order to be approved by security and distributed to the HUD-owned mobile IT device.
6. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel, of HUD-owned mobile IT devices.
7. Immediately report any lost or stolen HUD-owned mobile IT devices to the National Help Desk.
8. Return HUD-owned mobile IT devices that have been damaged or are no longer required to the OCIO.

9. Due to voice plan minute restrictions, employees should opt to use their work landline phone, when at their workstation, to make and receive calls.
10. Abide by the law governing the use of mobile cell phones and/or smartphones, for example while driving (*e.g.*, hands-free use and/or texting).
11. Notify and obtain approval from program authorized individual at least 30 days in advance of official international travel with HUD-owned mobile IT device.
12. Ensure that the HUD-owned mobile IT device is protected at all times from unauthorized access and is NOT used by any other user.
13. Comply with the provisions of the HUD Mobile IT Device guidance, including use of the device for official government use and limited personal use.

B. BYOD Mobile IT Device

Under BYOD program, the OCIO will provide leadership, guidance, and oversight in the establishment and maintenance of inventories; however, the device costs will be paid by the employee. HUD will respect the privacy of your personal device and will only request access to the device by technicians to implement security controls, as outlined below, or to respond to legitimate discovery requests arising out of administrative, civil, or criminal proceedings (applicable only if user downloads government email/attachments/documents to their personal device). This differs from policy for government-provided equipment/services, where government employees do not have the right, nor should they have the expectation, of privacy while using government equipment or services. While access to the personal device itself is restricted, HUD's Information Resource Management Handbook Policy and Rules of Behavior regarding the use/access of government e-mail and other government system/service remains in effect. Participation is voluntary but must be approved by management.. If there are questions related to compliance with the below security requirements, the user may opt to drop out of the BYOD program versus providing the device to technicians for compliance verification. The following section outlines the roles and responsibilities for OCIO, Program, and the employees who elect to participate in BYOD program.

B1. Office of the Chief Information Officer will:

1. Centrally negotiate, acquire, and manage the Mobile Device Management solution and licenses for the BYOD program that realizes cost efficiencies, ensures accountability and controls access to Departmental resources, and ensures compliance with federal technology and security standards.
2. Work with the Program and Support Office annually to adequately plan for software, licenses and needs for BYOD program participants during each budgetary cycle, as required by HUD's established IT Capital Planning process.
3. Identify the baseline number of BYOD mobile IT licenses to be funded, maintained, and supported by the OCIO. BYOD mobile IT devices requirements will be assessed

annually by the OCIO with input from the Program and Support Offices through the IT Capital and Acquisition planning processes. OCIO will provide information to the Program and Support Offices regarding BYOD program (i.e., current features, services, and associated costs) and management information (i.e., inventory listing and usage) to ensure effective and prudent use.

4. Distribute and manage the BYOD program software and licenses, in accordance to established IT Capital Planning and IT acquisition requirements.
5. Provide funding and support resources, as approved by the IT Capital Planning process, for BYOD program and its integration with the HUD network.
6. Ensure that BYOD program complies with all applicable HUD IT security policies and procedures. Take appropriate action (such as wiping) BYOD program device when required.
7. Develop and disseminate quarterly usage reports to ensure adequate and appropriate HUD-owned mobile IT device usage. OCIO reserves the right to terminate government-provided services for the BYOD for non-use. The policy for terminating voice and data services for non-use is 30 days.
8. Monitor and review BYOD program to ensure:
 - a. A sound understanding of BYOD program efforts across the Federal Government;
 - b. A proper balance between BYOD program requirements and customer feedback;
 - c. Compliance with regulatory requirements and standards for BYOD IT devices;
 - d. The optimal benefits are realized from investments in BYOD program.
9. Provide leadership, guidance, and oversight in the establishment and maintenance of the BYOD program.
10. Provide advice and assistance to Program and Support Offices regarding BYOD program to ensure effective and prudent use.
11. Periodically conduct surveys to ensure that BYOD management and services are being acquired at the most economical costs available.
12. Ensure that BYOD services are upgraded as required to provide reliable management capabilities.
13. Monitor and manage the level of availability, performance, and restoration for BYOD devices.

14. Annually provide reports to the Program and Support Offices regarding the participation in the BYOD program. Report will include information regarding the employee as well as the mobile device used in the program.
15. Ensure that principal and staff offices comply with the provisions of the HUD Mobile IT Device guidance, including use of the device for official government use, HUD Mobile Rules of Behavior and other applicable governing policies.
16. Provide basic BYOD solution training to approved BYOD users.

B2. Program and Support Offices will:

1. Establish the GDAS or designee for each Program and Support Office who will serve as the authorized individual for approving and submitting requests to the OCIO for employees who wish to participate in the BYOD program.
2. Submit approved requests for BYOD program to the OCIO through the GDAS or designee.
3. Identify business and program requirements and work with the OCIO to develop standardized, cost-effective solutions for the BYOD program.
4. Review the OCIO HUD-owned mobile IT device usage reports to ensure that the office is using these devices adequately and effectively, and take the necessary actions to eliminate redundant, unauthorized, or unused HUD-owned mobile IT devices.
5. Review the OCIO reports on the BYOD program to ensure that a bona fide business need exists for employees to participate in the program. In addition, program and support offices must identify any accounts to OCIO that should be terminated.
6. Include, as necessary, BYOD program requirements as part of the IT Capital Planning process.
7. Submit approved waiver requests to the OCIO for distribution of HUD-owned mobile IT devices to Fair Labor Standards Act (FLSA) covered employees, interns, or other non-government employees.
8. Notify OCIO of any separation, transfer, or termination from the Department of any employee participating in the BYOD program, so that OCIO can take the appropriate actions.
9. Confirm individuals participating in the BYOD program with the OCIO on an annual basis.
10. Ensure that the office and applicable employees comply with the provisions of this guidance and the signed Rules of Behavior for Connecting Mobile IT Personal Devices to HUD Resources.

B3. Employees will:

1. Complete the IT Security Awareness Training within the designated timeframe and understand the security risks associated with participating in the BYOD program,
2. Request BYOD program participation through the authorized individual in their respective Program or Support office.
3. Return existing HUD-owned mobile device to OCIO.
4. Sign, submit and comply with HUD's BYOD program Rules of Behavior and applicable policies.
5. Exercise extra care to preclude the compromise, loss, or theft of the device, especially during travel.
6. Immediately report any lost or stolen BYOD program device to the National Help Desk.
7. Notify the National Help Desk to be removed from the BYOD program or when leaving the Department.
8. Ensure that the BYOD program is protected at all times from unauthorized access and is NOT used by any other user. This provision applies only to the use of HUD resources and not the device.
9. Notify National Help Desk prior to upgrading or replacing and device participating in the BYOD program.
10. Provide BYOD program device to OCIO when requested and agree with BYOD device wiping when required. Wiping may include government data only or the entire device, when necessary.
11. Be responsible for all device and/or carrier service requests outside of the HUD BYOD software.
12. Be responsible for all payments required on the device, including the device and carrier service costs.
13. Abide by the federal and local laws governing the use of mobile cell phones and/or smartphones; for example, while driving (*e.g.*, hands-free use and/or texting)
14. Comply with the provisions of this guidance, including those detailed in the Rules of Behavior for Connect Mobile IT Personal Devices to HUD Resources.

11-6 ACQUISITION

Acquisition of HUD-owned mobile IT devices and services is centrally administered through OCIO. OCIO manages the BYOD program and technology needed and installed for participation.

- A. The OCIO is responsible for the acquisition and distribution of HUD-owned mobile IT devices for the Office of the Secretary, Senior Executive Service (SES), and approved Program and Support Office personnel. The OCIO will ensure anticipated HUD-owned mobile IT device requirements undergo appropriate IT Capital Planning and Acquisition processes, comply with all applicable Federal laws and regulations, and adhere to IT Security policies and procedures.
- B. Requests for HUD-owned mobile IT devices for departmental personnel other than the Office of the Secretary or SES personnel must be submitted to the OCIO by the authorized Program and Support Office personnel. Beginning in Fiscal Year (FY) 2012, the Program and Support Offices will be required to provide funding for the purchase and maintenance of mobile IT devices for departmental personnel that exceed their designated number of devices. Therefore, Program and Support Offices must ensure that anticipated HUD-owned mobile IT device requirements are identified in FY 2012 and all subsequent years, following the Department's established IT Capital Planning process.
- C. The OCIO is responsible for the acquisition and distribution of BYOD licenses for the Office of the Secretary, Senior Executive Service (SES), and Program and Support Office personnel. The OCIO will ensure anticipated BYOD requirements undergo appropriate IT Capital Planning and Acquisition processes and adherence to IT Security policies and procedures.