Office of the Chief Information Officer

Rules of Behavior for Connecting Mobile IT

Personal Device to HUD Resources

What is the Purpose of the Rules of Behavior for Connecting Mobile IT Personal Devices to HUD Resources?

The intent of these Rules of Behavior is to summarize laws and guidelines from various HUD and other Federal documents, most specifically OMB Circular A-130 and Section 208 of the E-Government Act of 2002. These guidelines should be used by all HUD Employees who volunteer to participate and are found eligible to participate in the Bring Your Own Device program. Additional information about Mobile Device Management is provided in the Information Resource Management Handbook 2400.1 Chapter 11.

What are Rules of Behavior?

Rules of Behavior are part of a comprehensive program to provide complete information security. These guidelines were established to hold users accountable for their actions and responsible for information security. Rules of Behavior establish standards of behavior in recognition of the fact that knowledgeable users are the foundation of a successful security program. Users need to understand that taking personal responsibility for the security of their computer and the data it contains is an essential part of their job.

Who is Covered by These Rules?

These rules extend to all HUD personnel who voluntarily participate in the Bring Your Own Device program. All users should be fully aware of, and abide by, HUD security policies as well as related federal policy contained in the Privacy Act, Freedom of Information Act, and HUD Records Management Regulations.

What is Sensitive Data?

Sensitive data is data that must be protected on the basis of the need for protection against loss, disclosure, or alteration because of the risk and magnitude of harm that could result.

What are the penalties for Non-compliance?

All users are required to comply with the Enterprise Rules of Behavior (http://hudatwork.hud.gov/po/i/it/security/documents/robguide.pdf). Additionally, those employees who voluntarily participate in the Bring Your Own Device program are required to comply with the additional rules identified in this document.

By signing the Rules of Behavior for Connecting Mobile IT Personal Devices, the employee indicates that s/he understand, accept, and agree to comply with all identified terms and conditions. Failure to comply with these rules could result in a verbal or written warning, removal of system access, termination of employment, and/or found guilty of a misdemeanor punishable by fines up to $5,000[1].

[1] "Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific

Bring Your Own Device (BYOD) Program Participants:

- Participation in the BYOD program is voluntary and can be terminated by the employee at any time. Participants assume all responsibility for device, accessories, and carrier service costs.
- Users shall adhere to the established HUD Enterprise Rules of Behavior and associated IT Security guidance and behave in an ethical, informed, and trustworthy manner.
- 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);
- Access to HUD IT resources via the BYOD program is in accordance with HUD's Information Technology Security Policy, Handbook 2400.25, Rev. 1 (to be referred to as the IT Security Handbook) HUD Personal Use policy (Section 4.6.6).
- Shall not attempt to override technical or management controls and/or configurations installed as part of the BYOD program.
- Shall take precautions to secure government information and information resources.
- Shall immediately report loss of the BYOD device to the National Help Desk for remote removal of the Mobile Device Management solution and redirection of e-mail.
- Shall notify National Help Desk prior to the disposal/upgrades of BYOD device(s).
- Shall physically protect BYOD device from theft, abuse and unauthorized use. Participants should be particularly aware of the threat of loss during periods of travel. HUD recommends using the general device password in addition to the HUD BYOD program password.
- Shall not copy government information onto personally-owned equipment.
- Shall protect passwords from access by other individuals, e.g., do not store passwords in login scripts, batch files, or elsewhere on the device.
- Shall report security incidents or any incidents of suspected fraud, waste or misuse of HUD systems to appropriate officials immediately.
- Shall complete the form below and scan/send the signed version to their management official.
- Shall ensure that the activation PIN, provided by HUD after completion of the form, enables access to the HUD resources.

Management Official:

- Shall ensure that Fair Labor Standard Act (FLSA) covered employees are not participating in the program without GDAS-level approval.
- Shall review authorizations annually to ensure that a bona fide business need exists for employees to participate in the program. In addition, management officials must identify any accounts to OCIO that should be terminated.
- Shall ensure that personnel granted participation in the BYOD program follow established HUD IT security policies, guidelines and procedures.
- 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.

---

material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000." 5 U.S.C. § 552a(i)(1).

Office of the Chief Information Officer
Rules of Behavior for Connecting Mobile IT Personal Device to HUD Resources

I certify I have read and understand the Department of Housing and Urban Development's Rules of Behavior for Connecting Mobile IT Personal Device to HUD Resources. I acknowledge, understand and will comply with the above-referenced security policy and rules of behavior, as applicable to my BYOD usage of HUD's services. By signing the Rules of Behavior for Connecting Mobile IT Personal Devices, I understand, accept, and agree to comply with all identified terms and conditions. Failure to comply with these rules could result in a verbal or written warning, removal of system access, termination of employment, and/or found guilty of a misdemeanor punishable by fines up to $5,000. I understand that participation in the BYOD program is voluntary and can be terminated at any time. I understand that addition of government-provided third party software may decrease the available memory or storage on my personal device. I understand that business use may result in increases to my personal monthly service plan costs. I will assume ALL responsibility for device, accessories, and carrier service cost and understand that government reimbursement of any business-related data/voice plan usage of my personal device is not provided. I understand that HUD is not responsible for any loss or theft of, damage to, or failure in the device that may result from use of third-party software and/or use of the device in this program. I understand that I must immediately report loss of the BYOD device to the National Help Desk for remote removal of the Mobile Device Management solution and redirection of e-mail. 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 HUD. In order to remain in the BYOD program, I must complete HUD's mandatory annual IT Security Training within the HUD Virtual University System (HVU system).

EMPLOYEE VOLUNTARY PARTICIPATION INFORMATION:

Employee Name (Print): _____ User ID (H#) : _____

Work Address and Phone Number (Print): _____

Requests access to the following systems/applications: _____

Employee Signature: _____ DATE:_____

Device Information (place an 'X" by the type of device - you may only check one device type. Enter the information about the particular device.):

_____ Smart Phone _____Device Brand Name

_____ Tablet _____Operating System and Version

Carrier _____

EMPLOYEE SUPERVISOR APPROVAL:

Supervisor Name (Print): _____ Phone Number:_____

Signature: _____ DATE: _____