Bring Your Own Device Policy and Procedure

Purpose: This policy describes the Agency's Bring Your Own Device Program (BYOD Program), which permits employees to use their personally-owned, approved mobile devices to access Agency email.

Scope: This policy applies to all Agency employees participating in the BYOD program.

Policy: DOHMH will allow Agency employees to participate in the BYOD Program and utilize their personally-owned, approved mobile devices to access Agency email, subject to Divisional Approver/Deputy Commissioner approval. Participation in the BYOD Program is completely voluntary: 1) The Agency will not compensate employees for any hardware costs or service carrier fees; 2) The Agency will not provide support or maintenance services; 3) If an employee uses his or her device to access DOHMH email or DOHMH applications outside of his or her regular work schedule, the employee will not be compensated for any additional time unless the employee is eligible to earn overtime compensation AND the device was being used in conjunction with pre-approved overtime. In addition, participating Programs and employees have the following responsibilities:

1. Usage: All usage while accessing Agency information is subject to the DOHMH Acceptable Use policy and all data transmitted is subject to investigation, F.O.I.L and legal discovery. Email may be read and sent, but files may only be viewed on the device. Saving or editing files is prohibited. Some users may experience some limitations in using other applications / features on their device while accessing Agency email.
2. Right to revoke: the Agency can at any time revoke, without prior notification, an employee's privilege to participate in the Program.
3. Release of liability and disclaimer: Participants in the BYOD Program acknowledge that using a personal device in connection with Agency business carries specific risks for which the employee assumes full liability. These risks include, but are not limited to, the partial or complete loss of personal data as a result of a crash of the OS, errors, bugs, viruses, and/or other software or hardware failures, or programming errors which could render a device inoperable.
4. Release of phone number: Participants are required to provide their cell phone number to DOHMH and keep it up-to-date, and authorize DOHMH to call for work and emergency notification purposes.
5. Approval: Participating employees are required to submit a Mobile Device Request form and agree to the BYOD policy by checking the check accept box on the MDR and their Divisional approver approval.
6. Approved devices: Only non-Windows operating system (OS) devices can be used (e.g., Android, and Apple products, excluding laptops). Devices that have had hardware or software modifications [e.g., jailbroken (Apple), rooted (Android)] are prohibited.

7. Device Enrollment: The agency's email administrator will send you an instruction to enroll your device to the DOHMH BYOD Management platform (MDM – Mobile Device Management). You must follow the instruction precisely in order to avoid losing your personal information once you either leave the agency or leave the BOYD program. DOHMH reserves the right to remotely wipe the agency's information from BYOD devices.
8. Fees: All costs associated with personally owned devices (e.g., the cost of the device, replacement, repairs, service carrier charges[1]) are the employee's responsibility.
9. Security: The following are required and recommended protections to safeguard Agency data:
    a. DOHMH implemented:
        i. Auto application logout – after five minutes of inactivity.
        ii. Auto wipe – after 10 incorrect log-in attempts, a device is reported lost or stolen, DIIT detects a data or policy breach or virus, or your employment at the Agency has terminated, the DOHMH email and access will be wiped remotely from the device.
    b. Employee implemented: Employees are strongly encouraged to implement these protections:
        i. Auto device lock – After five minutes of inactivity the device will be locked.
        ii. Auto wipe – after 10 incorrect password attempts, the device will be wiped of all data.
        iii. Back-up – periodically save all personal data
10. Loss or Theft: If a device is lost or stolen, the employee must immediately contact the DOHMH Service Request Center, either by phone or logging an IT Service Request (Email and Mobile Device > BYOD Lost/Stolen/Unregister) and notify your supervisor.

Procedures: Submit a Mobile Device Request:

- Select your Divisional Approver/DC.
- Select Bring Your Own Device (BYOD) under Mobile Device Ownership.
- After reading the BYOD Policy and checking the Accept box, select the type of phone (Android Phone, Apple Phone, or Tablet).
- Select your mobile phone number and mobile phone carrier.
- Click Submit & Closed. You will be emailed set-up instructions.
- To report your device has been lost or stolen, or terminate your participation in the BYOD program: Indicate the date of the loss/theft or your termination date (please submit an IT Service Request at least five days prior to your last day).
- To update your phone number: submit an IT Service Request and provide your new mobile phone number and mobile carrier (if needed).

1 Service carrier charges include all charges billed to you by your service provider. Please check with your service provider to see if you will incur any additional charges for receiving Agency email on your device.

Document Revision History:

Date	Description
August 2013	Modified
December 2017	Updated
July 23, 2019	Updated as per NTS
October 22, 2019	Published