Guidelines

Title:	ODHS|OHA 070-001-05 Mobile Operating System Upgrade Guidelines
Related to:	ODHS|OHA 070-001 Mobile Communication Devices
Effective date:	06/06/2022

Purpose

This document provides guidelines for updating operating systems on agency-owned or approved personal mobile communication devices (MCDs) in accordance with Office of Information Services (OIS) requirements. These guidelines apply to smartphones, iPads, and standard cellphone and firmware operating systems.

Guidelines

1. All device operating systems should have the authentic operating system software or firmware released by the device manufacturer. Users should not alter operating systems or firmware, also known as “jailbreaking” or “rooting” devices.
2. Individual users are responsible for ensuring that their device is running the most current operating system as they are released.
   a. Updates to the operating system may require the device to be plugged into power and connected to a Wi-Fi network.
   b. Devices will automatically connect to agency Wi-Fi when the device is in the office, however, remote workers may need to connect to an alternative network such as home Wi-Fi to receive operating system updates.
3. Installation of the operating system updates should be performed regularly and according to the update instructions. Users may ask their MCD coordinator, visit the OIS website, or contact the OIS Service Desk for these instructions.
4. Some older devices may not be capable of updating to newer operating systems.
   a. If a device is not able to update to the required operating system version, the device should be replaced with a newer model.
   b. The user completes the MSC 1496 form to have the device replaced with a newer model.
5. The allowed versions of levels of device operating systems should be determined by OIS based on alerts provided by the manufacturer, and in accordance with federal and state security requirements.
   a. Any agency-owned device that has an operating system below the allowed versions, may be restricted from accessing the agency’s information systems or may have their service interrupted until the issue has been corrected.
   b. The user will be notified by OIS prior to this restriction being applied.

References

ORS 182.122 Statewide Information Security Standards

Forms referenced

MSC 1496 Mobile Communication Device Order/Change Request Form

Related policies

ODHS|OHA 070-001 Mobile Communication Devices

Contact

Office of Information Services
Service Desk
(503) 945-5623
dhs.servicedesk@state.or.us

Guidelines history

Version 1 DHS|OHA established 3/19/15
Version 1 DHS|OHA reviewed with no changes 02/21/17
Version 1 ODHS|OHA reviewed with no changes 12/07/2020
Version 2 ODHS|OHA revised 06/06/2022

Keywords

Agency-owned MCDs, authentic operating system software, cell phones, cellular service, communication, corporate devices, device, encryption, firmware, hotspot, jailbreaking, line of service, MCD, Mi-Fi, mobile, mobile communication device, mobile communication device coordinator, mobile device management, MDM, OIS Collaborative Communications, rooting, smart phone, wireless.
