



**Maine State Government
Dept. of Administrative & Financial Services
Office of Information Technology**

Non-OIT Managed Mobile Device Policy

I. Statement

Mobile devices not supported by OIT, which are joined to the state network, must comply with this policy.

II. Purpose

Subject to certain provisos, OIT allows non-OIT managed mobile devices (non-OIT mobiles for short) to join the state network. Non-OIT mobiles include both devices acquired by state agencies but not managed by OIT, as well as personal devices acquired by state personnel.

III. Applicability

This policy establishes conditions under which non-OIT mobiles are allowed access to the state network.

IV. Responsibilities

A. Agency Management: (1) Approve requests for non-OIT mobiles to be connected to the state network. (2) Must notify OIT Customer Support as soon as possible regarding any transition (transfers, terminations, etc.) of non-OIT mobile holders.

B. Customer: Obtain management approval and submit a request to the Non-OIT Mobile Portal. Once configured for access, it is the customer's responsibility to provision the non-OIT mobile device with the appropriate client app or any other device-specific hardware/software required to access the State network.

C. OIT: Assist with the configuration of the non-OIT mobile to access the state network.

V. Directives

A. Operating systems supported include currently supported versions (by the original equipment manufacturer) of Google Android and Apple iOS.

B. Non-OIT mobiles are allowed one of two means for accessing state email & calendar: direct connection via Juniper VPN (Junos) and the Outlook Web Access (OWA). Either method

requires two-factor authentication via RSA SecurID token/pid, plus the employee's state Active Directory credential. Managed non-OIT mobiles are provided direct connectivity to the state wireless network, where available, and remote access through the state's Juniper VPN gateway.

C. OIT reminds all parties that all relevant State, Agency, and DAFS-OIT policies, including FOAA for State contents (Title 1, Chapter 13) and the Notice of Risk to Personal Data Act (Title 10, Chapter 210-B), continue to apply with respect to state I.T. resources, irrespective of whether such access is effected via an OIT device or a non-OIT device.

D. OIT further reminds all parties that State, Agency, and/or DAFS-OIT Acceptable Usage Policies apply while connected to the state network, irrespective of whether such access is effected via an OIT device or a non-OIT device. Consequently, even when the state network is accessed via a non-OIT device, H.R. Directors and Assistant Attorneys General may be allowed to initiate forensic audits on such devices, as well as to quarantine applications not relevant to state business from being operated while connected to the state network.

E. Should a device cease to be in the safe custody of the device holder (due to, but not limited to, loss or theft), device holders *must* notify OIT Customer Support as soon as possible to limit unauthorized access and data loss. Users are strongly urged to back up the contents of their mobile device, as lost devices used for state business are subject to being (remotely) wiped.

F. For security purposes, the following password requirements apply:

1. Device must be secured by a password, minimum eight characters long, with at least one character alpha and one numeric. A non-expiring password is acceptable.
2. The device must lock after a period of inactivity; fifteen minutes at a maximum.
3. Ten incorrect attempts at entering the device password will trigger a remote wipe.

G. Should the device store, even temporarily, Personally Identifiable Information, the device must be encrypted to the AES-256 standard.

H. Tampering with the original equipment manufacturer's standard security configuration (rooting, jail breaking, etc.) summarily disqualifies a device from using the state network.

I. All client-side product licenses are provisioned by the agency and/or the device holder. (OIT currently only provides the Junos Pulse license.)

J. For the purpose of access audit to state I.T. assets, the assumption is that each device has one, and only one, designated user. Non-OIT device user/holders hereby vouch that devices are not shared with any other person (including family members).

K. Agencies *must* notify OIT Customer Support as soon as possible regarding any transition (transfers, terminations, etc.) of non-OIT mobile holders.

L. Since non-OIT mobiles are not maintained by OIT, OIT's troubleshooting assistance can only be on a best-effort basis. Users will have to coordinate assistance from OIT and the wireless carrier, if applicable. The only OIT deliverable is access to the state network.

M. Should statutory restrictions forbid particular agency stakeholders from accessing specific state information assets from non-state devices, then this policy does *not* change that.

N. The state is held harmless for any damage to a personal device as a consequence of being used for state business and accessing the state network.

O. Failure to comply with any of the above provisos may lead to termination of access to the state network.

VI. Definitions

Non-OIT Managed Mobile Devices: Computing and/or communication devices, not managed by OIT, running a mobile operating system (such as Google Android, Apple iOS, Microsoft Windows RT, BlackBerry OS, etc.), as opposed to desktop-class operating system (such as Windows, Mac OS, Ubuntu, etc.).

VII. References

VIII. Document Information

Adoption Date: July 31, 2013

Effective Date: July 31, 2013

Update Date: July 31, 2013

Next Review Date: July 31, 2015

Point of Contact: Wayne Gallant, Associate CIO, Infrastructure, Office of Information Technology, 207-624-9424.

Approved By: James R. Smith, Chief Information Officer, Office of Information Technology, 207-624-7568.

Position Title(s) or Agency Responsible for Enforcement: Greg McNeal, Chief Technology Officer, Office of Information Technology, 207-624-7568.

Legal Citation: 5 M.R.S.A. Chapter 163 Section 1973 paragraphs (1)B and (1)D, which read in part, “The Chief Information Officer shall:” “Set policies and standards for the implementation and use of information and telecommunications technologies...” and “Identify and implement information technology best business practices and project management.”

Waiver Process: See the [Waiver Policy](#)¹.

¹ <http://maine.gov/oit/policies/waiver.htm>