OFFICE OF THE CHIEF TECHNOLOGY OFFICER

District of Columbia Government – Office of the Chief Technology Officer

Enterprise Mobile Device Management Policy

Policy Number:	**OCTO – 7006.1**	**Creation Date:**	4/22/2016
		Approval Date:	4/22/2016
Effective Date:	4/22/2016	**Revised Date:**	

1. **Scope/Applicability:** This Policy applies to all DC Agency Directors, Chief Information Officers, and Agency Telecommunications coordinators, their designees, the District of Columbia Chief Technology Officer, and all District of Columbia workforce members.

2. **Authority:** DC Official Code § 1-1401 et seq.

3. **Purpose:** This Enterprise Mobile Device Management Policy ("Policy") is intended to establish roles, responsibilities and standard practices with respect to the effective and efficient management of mobile device usage for conducting government business and accessing the District of Columbia ("DC") Government Network.

4. **Definitions:**

   4.1. "Government Network" means the District of Columbia secure wide area network and District of Columbia Government data and systems, including electronic mail (email).

   4.2. "Mobile Electronic Communications Device" or "Mobile Device" means any device used by subscribers and other users of wireless telephone service to access the wireless service. Mobile devices include cell phones, smart phones, tablets, rugged devices, netbooks or any other handheld device that allows access to wireless service.

   4.3. "Workforce Members" means DC government employees, contractors, volunteers, and temporary personnel authorized to use DC government-owned equipment and/or network resources.

5. **Policy:** Any DC Agency Director that allows DC workforce members to conduct government business and access the DC Government Network on a government-issued mobile device or a personal mobile device must comply with the following procedures. Any DC workforce member that conducts government business and accesses the DC Government Network on a government-issued mobile device or a personal mobile device must comply with the following directives.

   5.1. DC workforce members may only use government issued mobile devices or personal mobile devices for government business and/or to access the DC Government Network if a DC Agency Director or his/her designee authorizes such use. The form of the authorization is set forth in Section 5.3, below.

   5.2. The DC workforce member must download, install, and use an OCTO-approved third-party mobile device management application on the mobile device immediately after he or she is authorized to use the mobile device to conduct government business and/or to access the DC Government Network. DC workforce members must comply with Mayor's Order 2012-102, "Use of Private Email to Transact Public Business," and the "Electronic Mail Use Policy," OCTO Policy No. OCTO – 4040.2, when email systems and services provided by or owned by DC government are accessed, downloaded, installed, or used on any government-issued or personal mobile-device.

5.3. Roles and Responsibilities:

5.3.1. Each Agency Director and his/her designee must:

5.3.1.1. Require all District of Columbia workforce members to download, install, and use an OCTO-approved third-party mobile device management application on the government-issued mobile devices upon receipt of the government-owned mobile device.

5.3.1.2. Inform all District of Columbia workforce members that the use of personal mobile devices for government business is permitted only if: (1) the use is authorized by the Agency Director or his/her designee and (2) the DC workforce member downloads, installs, and uses an OCTO-approved third-party mobile device management application on the personal mobile device.

5.3.1.3. Require all DC workforce members he or she approves to use personal mobile devices to conduct government business or access the DC Government Network to download, install, and use an OCTO-approved third-party mobile device management application on the personal mobile device.

5.3.1.4. Require each District of Columbia workforce member who uses a government-issued or personal mobile device to conduct government business to review this policy and related procedures and acknowledge in writing that (1) compliance with the policy is a condition of using any mobile device to conduct government business or access the DC Government Network and (2) he or she consents to the installation and use of the OCTO-approved third-party mobile device management application on his or her personal device (if applicable).

5.3.2. Each Agency workforce member must:

5.3.2.1. Download, install and use an OCTO-approved third-party mobile device management application on their government-issued mobile device and any personal device used to conduct government business or access the DC Government Network;

5.3.2.2. Use a password to protect the government-issued mobile device and any personal device used to conduct government business or access the DC Government Network;

5.3.2.3. Acknowledge in writing that (1) compliance with the policy is a condition of using any mobile device to conduct government business or access the DC Government Network and (2) he or she consents to the installation and use of the OCTO-approved third-party mobile device management application on his or her personal device (if applicable).

5.3.3. OCTO must assist Agency Directors and their designees to implement and enforce this policy and must designate the OCTO-approved third-party mobile device management software or application that DC workforce members must download, install, and use on mobile devices used to conduct government business and/or access the DC Government Network.

5.4. DC government reserves the right to: (1) track any government-issued mobile device used by any DC workforce members that accesses the DC Government Network; (2) monitor the location of any government-issued mobile device that accesses the DC Government Network; and (3) restrict access to data and files on the government-issued mobile device. If DC government elects to install tracking features on any government-issued mobile device, the Agency Director issuing the device must notify the DC workforce member using the device, both verbally and in writing, that DC government is using a tracking feature on the government-issued mobile device.

6. **Procedures:** OCTO may create procedures in written or electronic form, in accordance with this policy, for DC Agency use and implementation.

7. **Policy Maintenance:** The Office of the Chief Technology Officer (OCTO) is responsible for the maintenance, administration, and publication of this policy. OCTO must annually review this policy and update as needed to ensure the policy's technical relevance and regulatory compliance.

8. **Policy Enforcement:** OCTO is responsible for the enforcement of this policy. Agencies must actively participate in the audit of this policy when requested by the OCTO.

9. **Exemptions:** None.

10. **Sanctions:** If OCTO discovers non-compliance with this policy, OCTO will:

    10.1. Advise the DC Agency CIO of the non-compliance and assist the DC Agency CIO in developing a corrective action plan and a reasonable timeframe for its implementation.

    10.2. If the DC Agency CIO does not implement the corrective action plan within the stated timeframe, OCTO will escalate the matter to the DC Agency Director for immediate action and resolution.

    10.3. If the DC Agency Director does not resolve the policy non-compliance within his/her DC Agency, OCTO will refer the matter to the DC City Administrator for immediate action and resolution.

11. Related Orders, Regulations, and Policies:

11.1. Title 6B of the DC Municipal Regulations;
11.2. Mayor's Order 2012-102, "Use of Private Email to Transact Public Business";
11.3. Landline Telephone and Mobile Electronic Communications Device Usage Procedures (OCTO – 7006.1);
11.4. Virtual Private Network Policy (OCTO – 2060.2);
11.5. Password Management Policy (OCTO – 2003.2);
11.6. Telecommunications Service Acquisition Policy (OCTO – 1072.0);
11.7. Electronic Mail Use Policy (OCTO - 4040.2).

12. **Policy Review:**

Document History

Policy Number	Action	Effective Date	Next Review Date
OCTO – 7006.0	Created	2/2/2016	2/2/2016
OCTO – 7006.1	Published	4/22/2016	4/22/2017

13. **Policy Acceptance:**

Enterprise Mobile Device Management Policy

Effective April 22, 2016

Archana Vemulapalli 4/22/16

Archana Vemulapalli
Chief Technology Officer
Government of the District of Columbia

Date