IT/IM DIRECTIVE PROCEDURE

Mobile Computing Management Procedures

Directive No: CIO 2154-P-01.3

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 07/07/2005

Mobile Computing Management Procedures

1. PURPOSE

These procedures establish requirements for implementing and managing the use of government furnished information management and technology solutions.

2. SCOPE

This procedure applies to government furnished information management and technology solutions that store, process, transmit or receive EPA information, such as laptops, tablets, smartphones, mobile management tools and other portable media devices that may be used at locations outside of EPA's secured network and physical environment. Senior Information Officials (SIOs) are responsible for implementing this procedure within their organization. This means SIOs must develop and maintain guidance and Standard Operating Procedures (SOPs) to implement the management controls described in Section 6.2 (Mobile Computing Management Controls) within their organization.

3. AUDIENCE

The audience for these procedures includes EPA employees, managers, contractors and grantees that use or manage mobile computing information management technologies and resources.

4. BACKGROUND

EPA and other Federal Agencies are challenged to create an environment that promotes transparency and workforce connectivity to enterprise resources while remaining secure. Employee work environments transcend the physical location of their duty station. In order to support this environment, EPA employees who manage or use government-owned and/or government furnished information management and technology solutions are responsible for following requirements set forth in EPA's information technology (IT) and information management (IM) policies, procedures and standards.

5. AUTHORITY

- EPA Telework Policy (PDF)
- Telework Enhancement Act of 2010, (H.R. 172), Public Law 111-292
- E-Government Act of 2002, (H.R. 2458), Public Law 107-347
- Mobile Computing Policy, EPA Classification No. CIO 2154.3

- Software Management and Piracy Policy, EPA Classification CIO No. 2104.0
- Privacy Policy, EPA Classification No. CIO 2151.0
- Flexiplace Policy, EPA Order 3180
- Executive Order 13589, Promoting Efficient Spending

6. PROCEDURES

6.1 Eligibility, Acquisition and Inventory

Eligibility - EPA employees and contractors whose duties require constant and immediate access to EPA email and/or Intranet may request to use certain mobile devices (e.g., handheld devices, smartphones, tablets). Employees must submit their request to receive, upgrade or replace a mobile device along with a business justification to their manager for consideration. These mobile devices should only be used to perform official government duties except as described in the EPA Limited Personal Use Policy. The authority to approve employee requests to use EPA managed handheld mobile devices is delegated to EPA Senior Information Officers (SIOs). SIOs can delegate this authority to program managers within their office.

Acquisition - EPA approved standard mobile devices can be found at the EPA IT Standards Profile site which provides a list of all approved mobile devices. The authority to manage the costs of acquiring mobile devices is delegated to the SIOs. SIOs may delegate this responsibility to a program manager within their organization.

Inventory - Program Offices and Regions must record and identify the individuals responsible for managing EPA managed mobile device components by name, position and role. Also, Program Offices and Regions must annually inventory EPA managed mobile devices deployed in their organizations. The mobile device inventory must include the information below, as well as other information deemed necessary by the organization to achieve effective property management and accountability. This information must be verified and confirmed for accuracy on a quarterly basis.

- Account Holder Responsibility Center (AHRC)
- Manufacturer
- Type
- Model
- Serial number
- Physical location
- Network component/device machine name or network address
- User name
- Date device issued and returned

6.2 Mobile Computing Management Controls

Program Offices and Regions must develop, maintain and utilize Standardized Operating Procedures that support the following activities:

- Verifying and confirming accuracy of the users' mobile device registration and utilization information in eBusiness on a quarterly basis.

- Developing business case justifications for the issuance of mobile devices.
- Developing a process to be used as a guide to determine appropriate consequences when inappropriate use of a mobile device is determined.
- Monitoring mobile device data and cell usage.
- Developing a process to review zero usage of mobile devices and business justification to determine whether a device should be terminated.
- Notifying users of the procedures to return their mobile device.

7. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO) is responsible for ensuring implementation of these procedures throughout the Agency.

Director, Office of Information Technology Operations (OITO) is responsible for:

- Overseeing policy and procedure implementation regarding use of mobile computing technologies.
- Approving mobile computing technology and device deployment.

Senior Information Officials (SIOs) are responsible for:

- Implementing these procedures within their organization.
- Making written determinations, concerning all requests to access sensitive PII from a remote location or take sensitive PII off site.
- Developing and maintaining guidance and Standard Operating Procedures (SOPs) to implement the management controls described in Section 6.2 (Mobile Computing Management Controls) within their organization.
- Approving authority for purchase and use of mobile devices within their office) and are responsible for carrying out procedures that support compliance with the procedure within their office. This authority can be delegated to Information Management Officers (IMOs) and Senior IT Leaders (SITLs).

Agency Privacy Officer is responsible for:

- Developing and implementing Agency level privacy policies, procedures, standards and guidelines.
- Conducting privacy on-site reviews to ensure compliance with the requirements to protect PII.

Information Management Officers (IMOs) are the approving authority for purchase and use of mobile devices within their office and are responsible for carrying out procedures that support compliance with the procedure within their office when authority is delegated by the Senior Information Official. IMOs are also responsible for addressing questions and concerns related to any implementation issues inherent in these procedures.

Program Offices and Regions are responsible for**:**

- Creating and maintaining an inventory of their IT equipment including mobile devices. The inventory must track both software and hardware procurements and include acquisition dates, property descriptions, associated licensing information and serial numbers for all items.

- Verifying and confirming the accuracy of registrations and utilization of mobile devices on a quarterly basis.
- Ensuring mobile devices are used in accordance with the Agency Personal Use Policy and Rules of Behavior and securing equipment to prevent unauthorized use and theft.
- Reporting all security incidents to the Information Security Officer for their organization, management and EPA Call Center.
- Complying with EPA Information Technology Standard EPA Enterprise Architecture (EA) standards.
- Ensuring end users comply with the provisions of these procedures.
- Reporting any and all security incidents to the Computer Security Incident response Center (CSIRC).
- Monitoring compliance with established EPA privacy and security policies, procedures, standards, Federal regulations, other applicable mandates and periodically reviewing internal control processes.

Working Capital Fund Managers are responsible for:

- Submitting an eBusiness order requesting mobile devices.
- Cancelling or reassigning mobile devices for their respective office.
- Conducting overall lifecycle management of mobile devices issued by the Government for their specific office and ensuring accurate billing and usage of each account.

Information Security Officers (ISOs) are responsible for:

- Ensuring Program Offices and individuals throughout their Program or Regional Office are cognizant of security and privacy requirements.
- Receiving notification and addressing questions, concerns and incidents related to any security issues.
- Reporting security incident findings to EPA Computer Security Incident Response Center (CSIRC).

Managers and Supervisors are responsible for:

- Approving the issuance of mobile devices.
- Addressing incidents of inappropriate use and non-compliance with these procedures.
- Answering questions from employees regarding this procedure.

Users are responsible for**:**

- Obtaining necessary approvals for the issuance of mobile devices.
- Complying with the Agency Personal Use Policy, Rules of Behavior and the procedures noted in the Mobile Device Acknowledgement Form regarding the appropriate use and protection of all EPA-owned or managed mobile devices. Being aware of information security requirements associated with the use of mobile devices.
- Ensuring the physical security of mobile devices (e.g., do not check with luggage or leave unattended, use a locking device).
- Turning off wireless access on mobile device (laptop, smartphone, tablet etc.) when not in use.

- Contacting their ISO and the EPA Call Center in the event a mobile device is lost or stolen.
- Contacting their ISO and the EPA Call Center in the event of an information breach.

8. RELATED INFORMATION

- Mobile Device (MD) Admin Responsibilities. This site provides a list of key MD Admin responsibilities.
- Mobile Device Website. This site provides general information about the use of agency mobile devices.
- EPA Personal Property Policy and Procedures Manual. The Manual presents policy and procedural guidance on personal property management issues for EPA employees and contractors.
- LAN Operating Procedures and Standards (LOPS). The LOPS manual provides a reference for LAN implementation and operation within the EPA's standardized framework.
- Responding to Personally Identifiable Information (PII) Breach Procedure, EPA Classification No. CIO 2151-P-02.4. This document establishes the requirements for responding to suspected or confirmed breaches of personally identifiable information (PII).
- Information Security-National Rules of Behavior. This document provides general instructions on the appropriate use of EPA information and information systems.
- EPA Travel Manual 2550B. This manual provides EPA Travel policy and procedures.
- International Travel Procedure for Mobile Devices. This procedure establishes requirements for mobiles devices used for international travel.
- Enterprise Architecture Procedures. These documents establish EPA's enterprise architecture requirements for EPA managed IT/IM solutions.
- Interim Records Management Policy, EPA Classification No. CIO 2155.4 This policy establishes principles, responsibilities, and requirements for managing EPA's records to ensure EPA is in compliance with Federal laws and regulations.
- Mobile Device Acknowledgement Form. This form outlines the procedures required by all EPA staff, including contractors, when using an Agency mobile device.
- SIOs, IMOs, and SITLs This document provides a list of Senior Information Officials, Information Management Officers and Senior Information IT Leaders.

9. DEFINITIONS

AHRC Code - Office Account Holder Responsibility Center is a code that can be alphanumeric which is used to provide a unique identifier for each organization within EPA. AHRC codes are available by contacting your Responsible Program Implementation Office (RPIO) Coordinator, Senior Budget Officer (SBO) or your Working Capital Fund Service Agreement Originator.

Alternate Work Site - A location other than the official duty station that is approved by the personnel's supervisor (e.g., residence, satellite office, flexiplace) in order to conduct EPA official business job duties.

eBusiness - EPA's information system used for ordering and billing Working Capital Fund services.

EPA Network - A system containing any combination of EPA computers, computer terminals, printers, audio or visual display devices, or telephones interconnected by telecommunication equipment or cables.

Flexiplace (Flexible Workplace) - Employment at a location such as a satellite location or employee residence during an agreed-upon portion of an individual's workweek.

Government Furnished Information Management and Technology Solutions - IT infrastructure consisting of hardware, software, networks, telecommunications, and services commonly used across the Agency regardless of location, mission, program or project.

Information - Any communication or representation of knowledge such as facts, data, or opinions in any medium or form, including textual, numerical, graphic, cartographic, narrative or audiovisual forms.

Information Technology - Any equipment or interconnected system or subsystem of equipment, that is used in the automated acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission or reception of data or information by an executive agency. For purposes of the preceding sentence, equipment is used by an executive agency if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency which (i) requires the use of such equipment, or (ii) requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services) and related resources. The term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract. The term "information technology" does not include national security systems as defined in the Clinger-Cohen Act of 1996 (40 U.S.C. 1452).

Laptop - A personal computer for mobile use. A laptop integrates most of the typical components of a desktop computer, including a display, a keyboard, a pointing device (a touchpad, also known as a trackpad, and/or a pointing stick) and speakers into a single unit. A laptop is powered by mains electricity via an AC adapter, and can be used away from an outlet using a rechargeable battery. The term "laptop" also refers to a number of classes of small portable computers such as Notebooks, Rugged, etc.

Mobile Device - A mobile device (also known as a handheld device, handheld computer or simply handheld) is a small, handheld computing device, typically having a display screen with touch input and/or a miniature keyboard and weighing less than 2 pounds (0.91 kg). Mobile devices include, but are not limited to, mobile computers, mobile internet device, mobile Web Smartphone, tablet computer, personal digital assistant/enterprise digital assistant, calculator, portable media player, digital still camera, digital video camera (or digital camcorder), mobile phone, smartphone, feature phone, pager and personal navigation device.

Portable Media Device - A highly portable device that can be inserted into and removed from an information system and are used to store text, video, audio and image information. Examples include portable external hard disks, zip drives, CDs, DVDs and USB drives. USB drives can also be referred to as thumb drives, flash drives, mini drives, micro vaults, memory sticks, pen drives or jump drives.

Personally Identifiable Information - PII refers to information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc.

RPIO - The Responsible Program Implementation Office code is a static number that is generally used for account purposes to provide a unique identifier for each organization within EPA.

10. WAIVERS

No waivers are accepted from the requirements of this procedure.

11. MATERIAL SUPERSEDED

Interim Mobile Computing Management Procedures, CIO-2150.4-P-01.2, February 2020

12. CONTACTS

For more information on this procedure, contact your Information Management Officer or Information Security Officer. You may also contact the Office of Mission Support, Office of Information Technology Operations.

VAUGHN NOGA

Digitally signed by VAUGHN NOGA
Date: 2020.11.13 10:10:28 -05'00'

Vaughn Noga
Deputy Assistant Administrator for Environmental Information and Chief Information Officer
U.S. Environmental Protection Agency