IT/IM DIRECTIVE POLICY

Mobile Computing Policy

Directive No: CIO 2154.3

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

Mobile Computing Policy

1. PURPOSE

This mobile computing policy establishes guiding principles and a framework for the Environmental Protection Agency (EPA or Agency) approach to complying with the Telework Enhancement Act of 2010. The primary purpose of this policy is to ensure mobile computing equipment and resources accessing the EPA network are managed and used appropriately while promoting resource saving, improved sustainability, employee recruitment and retention, as well as supporting continuity of operations.

2. SCOPE

This policy 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 policy within their organization. This means SIO's must develop and maintain guidance and Standard Operating Procedures (SOPs) for their organization to implement the management controls as described in Mobile Device Procedures Section 6.2 (Mobile Computing Management Controls) within their organization.

3. AUDIENCE

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

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, including employee work environments that transcend the physical location of their duty stations. Mobile computing allows employees to leverage information management and technology resources from locations outside of EPA's secured network and physical location. EPA must also effectively manage mobile resources to promote efficient spending of funds allocated for information technology needs. In order to support this environment, EPA employees who manage or use government furnished information management and technology solutions are responsible for following requirements set forth in the EPA 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 Office of Management and Budget (OMB) Memorandum M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines
- E-Government Act of 2002, (H.R. 2458), Public Law 107-347
- Executive Order 13589, Promoting Efficient Spending, November, 2011

6. POLICY

EPA employees, managers, contractors and grantees must manage and use mobile computing resources in accordance with applicable Federal and Agency information technology and management laws and policies. EPA's policies and procedures must support the use of mobile technologies to achieve access to EPA information and resources in an environment that complies with EPA enterprise architecture and security requirements.

6.1 Mobile Computing Requirements

EPA employees or other users who are granted permission to use EPA's network must use government furnished information management and technology solutions to access EPA's network outside of EPA's secured physical location (e.g. telework status, official travel.)

EPA Owned or Managed Mobile Resources must be:

- Consistent with and adhere to Agency information technology and operational policies, procedures and standards.
- Configured to protect EPA information: when in use by authorized persons; when connected to the EPA network; when connected to a network other than an EPA network; and in the event of loss or theft.
- Tracked and accounted for to ensure proper acquisition, upgrade and disposal; and monitored for authorized and unauthorized use.
- Assessed and inventoried to establish controls to monitor usage of mobile devices, software and services.

7. ROLES AND RESPONSIBILITIES

Chief Information Officer (CIO) is responsible for ensuring implementation of this policy 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 this policy within their organization.
- Granting authority to remotely access, transmit or transport PII.
- 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 as described in Mobile Device Procedures 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 requirements to protect PII.

Information Management Officers (IMOs) are responsible for:

- Approving and tracking purchase and use of mobile devices within their office.
- Carrying out procedures that support compliance with this policy within their office.
- Addressing questions and concerns related to any implementation issues inherent in this policy.

Information Security Officers (ISOs) are responsible for:

- Ensuring Program Offices and individuals throughout their organizations are cognizant of security and privacy requirements.
- Addressing questions and concerns related to security related issues for mobile computing devices.
- Reporting security incident findings to EPA Computer Security Incident Response Center (CSIRC).

Deputy Ethics Officials are responsible for addressing questions and concerns from employees related to any ethics-related issues inherent in this policy.

Managers and Supervisors are responsible for:

- Approving issuance of mobile computing devices.
- Addressing incidents, inappropriate use and non-compliance with this policy.
- Answering questions from employees regarding this policy.

Users are responsible for**:**

- Complying with the Agency Personal Use Policy and 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 use of mobile computing resources.
- Ensuring physical security of mobile computing devices (e.g., do not check with luggage or leave unattended, use a locking device).
- Contacting the ISO and the EPA Call Center in the event a mobile computing device is lost or stolen.
- Contacting the ISO and EPA Call Center in the event of an information breach.

8. RELATED INFORMATION

The following documents cover topics related to this Policy:

- 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. This manual presents policy and procedural guidance on personal property management issues for EPA employees and contractors.
- 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.
- Mobile Device Acknowledgement Form. This form outlines the procedures required by all EPA staff, including contractors, when using an Agency mobile device.
- Privacy Policy, EPA Classification No. CIO 2151.1. This document establishes Agency requirements for safeguarding the collection, access, use, dissemination and storage of (PII) and Privacy Act information in accordance with the Privacy Act of 1974.
- Limited Personal Use of Government Office Equipment Policy, EPA Classification No. CIO 2101.1. This document establishes Agency requirements that allow limited personal use of EPA managed resources.
- Protecting Sensitive Personally Identifiable Information (SPII) CIO 2151-P-10.0 This document ensures adequate protection of Sensitive Personally Identifiable Information (SPII): a) from inadvertent disclosure when collecting, accessing and disclosing it to authorized personnel; b) when being accessed from outside the Agency; c) when removed physically from an EPA location for authorized and approved purposes; and d) when maintained within the Agency.

- 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.
- SIOs, IMOs, and SITLs This document provides a list of Senior Information Officials, Information Management Officers and Senior Information IT Leaders.

9. DEFINITIONS

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

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. 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.

10. WAIVERS

No waivers will be accepted from the requirements of this policy.

11. MATERIAL SUPERSEDED

Interim Mobile Computing Policy, CIO 2154.2, February 2020

12. CONTACTS

For more information on this policy, 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 10:09:18 -05'00'

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