PREFACE TO SELECTED INFORMATION DIRECTIVES

CIO Transmittal No.: 15-010	CIO Approval Date: 06/12/2015

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

CHIEF INFORMATION OFFICER MEMORANDUM

SUBJECT: Chief Technology Officer (CTO) Responsibilities in Selected Information Directives

Re-assigned CTO responsibilities

Effective immediately, CTO responsibilities detailed in the selected information directives (i.e., Information Policies, Procedures, Standards, and Guidance) listed in Appendix A are re-assigned to the OEI Office of Technology, Operations, and Planning (OTOP) Director and the Senior Agency Information Security Officer (SAISO) as detailed. The re-assignment does not change any requirements in the selected information directives.

The OEI Information Directives Program Manager is directed to attach this memorandum and Appendix A as a Preface to each of the Information Directives listed. OEI will then update the Roles and Responsibilities section of each Information Directive in accordance with the normal review and update cycle.

Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

APPENDIX A

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2104.1 Software Management and Piracy Policy	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy and manage enterprise software licenses.	OTOP Director
CIO 2104-P-01.0 Software Management and Piracy Procedure	Provide procedures, standards, and guidance to senior level managers to: support the Agency's Software Management and Piracy Policy, manage enterprise software licenses, and provide covered users within their office with training and awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.	OTOP Director
CIO 2121.1 System Life Cycle Management (SLCM) Policy	Establish and publish procedures, technical operational procedures and standards (TOPS), and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2121-P-03.0 SLCM Procedure	Establish and publish procedures, TOPS, and guidance supporting the Agency's SLCM Policy. Review and approve waivers to the SLCM Procedure.	OTOP Director
CIO 2122.1 Enterprise Architecture (EA) Policy	Issue procedures, guidance, and technical standards associated with the EA with a specific focus on the technology architecture, chair the Quality Technology Subcommittee (QTS), and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-01.1 EA Governance Procedures	Issue procedures, guidance, and technical standards associated with the EA, with a specific focus on the technology architecture, chair the QTS, and review technology and security considerations in the Enterprise Target Architecture and Enterprise Transition Plan.	OTOP Director
CIO 2122-P-03.0 Information Technology Infrastructure Standard Procedure	Recommend to the CIO a specific IT standard, product or specification to be added to the official Agency IT Standards Profile with consultation from the Quality Information Council (QIC) and the QTS, and develop and maintain the Agency's Technology Architecture.	OTOP Director
CIO 2122-S-02.0 Personal Computer Configuration and Management Standard	Review and approve requests for waivers in regard to this standard.	OTOP Director
CIO 2123.1 Configuration Management Policy	Provide procedures, standards, and guidance to senior level managers in support of the Agency's Configuration Management Policy; institute change management processes; and provide a change management database.	OTOP Director

Information Directive	Prior CTO Responsibilities	Re-assignment
CIO 2150-P-01.1 Information Security - Interim Access Control Procedures	Approve all methods of dial-up access, approve all wireless connections, establish, document, authorize, and monitor all methods of remote access to an information system; delegate to Regions and other entities, as appropriate; and address co-management responsibilities for the Agency Security Architecture.	OTOP Director
CIO 2150-P-08.1 Information Security - Interim Incident Response Procedures	Determine Operational Status Categories during Alerts and Risks (OSCAR) 5 level (page 7).	SAISO
	Be available when the Computer Security Incident Response Capability (CSIRC) must report and coordinate incidents (page 16). Be available to meet with the Director of Cyber Security Staff (CSS) when senior managers are informed of incidents, occurrences and their status (page 18).	OTOP Director
CIO 2150-P-14.1 Information Security - Interim Risk Assessment Procedures	Approve the use of and, as appropriate, acquire and deploy enterprise vulnerability management technology. Consult with the SAISO to determine the coverage and compliance of enterprise vulnerability management technology with respect to federal and Agency requirements, including use of these tools to meet assessment requirements of other control families in NIST 800-53A, Revision 1, and to ensure the most cost effective, complete and accurate results.	OTOP Director
CIO 2150-P-15.1 Information Security - Interim System Services Acquisition Procedures	For the procurement of external information system services where a sufficient level of trust cannot be established, be available to confer regarding risks associated with the network and the Agency.	OTOP Director
CIO 2150-P-16.1 Information Security - Interim System and Communications Protection Procedures	Approve use of mobile VoIP-enabled units.	OTOP Director
CIO 2150.4 Mobile Computing Policy	Oversee policy and procedure implementation regarding use of mobile computing technologies. Approve mobile computing technology and device deployment.	OTOP Director
CIO 2150-P-01.1 Mobile Computing Management Procedures	Oversee policy and the implementation of the procedures. Approve enterprise mobile device types to be deployed. Review and approve requests for waivers in regards to the procedures.	OTOP Director

EPA INFORMATION PROCEDURES

EPA Classification No.: CIO-2150.4-P-01.1	CIO Approval Date: 12/06/2013
CIO Transmittal No.: 13 – 012	Review Date: 12/06/2016

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 AND APPLICABILITY

These procedures apply to government furnished information management and technology solutions that store, process, transmit or receive EPA information, such as laptops, handheld mobile devices smartphones, mobile management tools and software, network infrastructure, personal digital assistants and other portable media devices that may be used at locations outside of EPA's secured network and physical environment.

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

- 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-2150.4,
- Environmental Protection Agency Information Security Policy , EPA Classification No. CIO 2150.3
- Limited Personal Use of Government Office Equipment Policy, EPA Classification No. CIO 2101.0
- System Life Cycle Management Policy, EPA Classification CIO No. 2121.1
- Software Management and Piracy Policy, EPA Classification CIO No. 2104.0
- Enterprise Architecture Policy, EPA Classification No. CIO 2122.1
- Privacy Policy, EPA Classification No. CIO 2151.0
- Flexiplace Policy, EPA Order 3180
- President Barack Obama Memorandum, "Building a 21st Century Digital Government", May, 2012
- Digital Government Strategy: Building a 21st Century Platform To Better Serve the American People, May 2012

- Executive Order 13589, Promoting Efficient Spending
- Office of Management and Budget (OMB) Memorandum M-11-20, Implementing Telework Enhancement Act of 2010 IT Purchasing Requirements

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.

- Reporting mobile device business case justifications annually.

- Developing an upgrade and replacement schedule.

- Developing a standardized mobile device accessory list that addresses the number and type of accessories available for purchase.

- Tracking accessory costs.

- 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. RELATED DOCUMENTS

The following documents cover topics related to these procedures:

- 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.
- Office of Management and Budget (OMB) Memorandum M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines. This memorandum establishes requirements for Agencies to implement security telework policies.
- Office of Management and Budget (OMB) Memorandum M-11-20, Implementing Telework Enhancement Act of 2010 IT Purchasing Requirements. This memorandum establishes requirements regarding policies and purchase of Information technology that support Telework.
- Office of Management and Budget (OMB) Memorandum M-06-16, Protection of Sensitive Information. This directive provides a checklist for the protection of remote information.
- Office of Management and Budget (OMB) Memorandum M-07-16, Safeguarding Against and Responding to the Breach of Personally Identifiable Information. This memorandum requires agencies to develop and implement a breach notification policy.
- Guidance for Rules of Behavior in Information Security Plans. This document establishes the rules of behavior for users of EPA owned and managed equipment and resources.
- Procedures for Responding to Breaches of Personally Identifiable Information, EPA Classification No. CIO 2151-P-02.2. This document establishes the requirements for responding to suspected or confirmed breaches of personally identifiable information (PII).

8. ROLES AND RESPONSIBILITIES

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

Chief Technology Officer (CTO) and Director, Office of Technology Operations and Planning (OTOP) is responsible for:

- Overseeing policy and the implementation of these procedures.
- Approving enterprise mobile device types deployed.
- Reviewing and approving requests for waivers in regards to these procedures.

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.

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 (excluding enterprise mobile devices) and are responsible for carrying out procedures that support compliance with the procedure within their office. 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 exclusively by authorized EPA users for the performance of official Agency business 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 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 and Rules of Behavior in regard to 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 for laptops 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.

9. DEFINITIONS

AHRC Code - Office Account Holder Responsibility Center is a code that can be alpha-numeric 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.

Personal Digital Assistant (PDA) - A mobile device that functions as a personal information manager. Current PDAs often have the ability to connect to the Internet. A PDA has an electronic visual display, enabling it to include a web browser but some newer models also have audio capabilities, enabling them to be used as mobile phones or portable media players. Many PDAs can access the Internet, intranets or extranets via Wi-Fi or Wireless Wide Area Networks.

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

Waivers may be granted by the Chief Technology Officer. Program Offices and Regions must submit a waiver in accordance with the EPA IT Waiver Standard Operating Procedure.

11. RELATED PROCEDURES, STANDARDS AND GUIDANCE

The following documents cover topics related to this Procedure:

- 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.
- Standards of Ethical Conduct for Employees of the Executive Branch. Provides the principles of ethical conduct for Federal employees.

- EPA Travel Manual 2550B. This manual provides EPA Travel policy and procedures.
- International Travel Procedures for Mobile Devices, EPA Classification No. CIO-2150.3-P-18.1. This procedure establishes requirements for mobiles devices used for international travel.
- Interim Records Management Policy, EPA Classification No. CIO 2155.2. This policy establishes principles, responsibilities, and requirements for managing EPA's records to ensure EPA is in compliance with Federal laws and regulations.
- Procedure for Responding to Breaches of Personally Identifiable Information (PII), EPA Classification No. CIO 2151-P-02.2. This procedure identifies the steps the EPA will take to respond to suspected or confirmed breaches of personally identifiable information (PII). This procedure sets out the roles and responsibilities for reporting and responding to PII breaches so that Agency officials, employees and other individuals will be able to quickly and effectively respond to any breach for which the EPA is responsible.
- NIST Special Publication (SP) 800.53 Revision 4 (or later). Provides security and privacy controls for federal information systems and organizations. The purpose of this document is to describe security and privacy controls for federal information systems.
- Enterprise Architecture Procedures. These documents establish EPA's enterprise architecture requirements for EPA managed IT/IM solutions.
- System Life Cycle Management Procedures EPA Classification No. CIO 2121-P-03.3. This document establishes EPA's approach and practices in the pre-definition, definition, acquisition/development, implementation, operations and maintenance, and termination of EPA IT systems and applications.
- Mobile Security Reference Architecture. This document provides the Federal reference architecture for mobile computing.

12. MATERIAL SUPERSEDED

N/A

13. ADDITIONAL INFORMATION

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

Renee P. Wynn
Acting Assistant Administrator for Environmental Information
and Chief Information Officer
U.S. Environmental Protection Agency