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

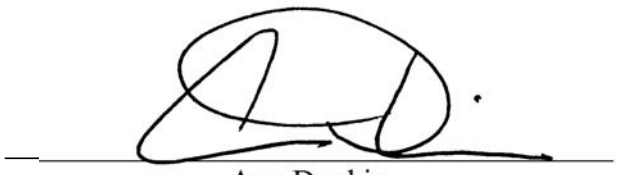
CHIEF INFORMATION OFFICER MEMORANDUM

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 POLICY

EPA Classification No.: CIO-2150.4	CIO Approval Date: 12/06/2013
CIO Transmittal No.: 13 – 013	Review Date: 12/06/2016

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 AND APPLICABILITY

This policy applies 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 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

- 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

- Office of Management and Budget (OMB) Memorandum M-11-20, Implementing Telework Enhancement Act of 2010 IT Purchasing Requirements
- 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
- E-Government Act of 2002, (H.R. 2458), Public Law 107-347
- Standards of Ethical Conduct for Employees of the Executive Branch, promulgated by the Office of Government Ethics
- 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 polices 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 and adherent to Agency information technology and operational policies, procedures and standards.
- Configured to protect EPA information: when in use by authorized or unauthorized 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. RELATED DOCUMENTS

The following documents cover topics related to this Policy:

- EPA Personal Property Policy and Procedures Manual. This manual presents policy and procedural guidance on personal property management issues for EPA employees and contractors.
- Office of Management and Budget (OMB) Memorandum M-11-27, Implementing the Telework Enhancement Act of 2010: Security Guidelines. This memorandum establishes security requirements for Federal 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 the 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.

- Enterprise Architecture Policy, EPA Classification No. CIO 2122.1. This document establishes EPA's Enterprise Architecture Program.
- Environmental Protection Agency Information Security Policy, EPA Classification No. CIO 2150.3. This document establishes a security policy for EPA.
- Information Security Procedures. These documents establish security procedures for the EPA network and information.
- Procedures for Responding to Breaches of Personally Identifiable Information (PII), 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).
- Guidance for Rules of Behavior in Information Security Plans. This document establishes the rules of behavior for users of EPA managed equipment and resources.
- Privacy Policy, EPA Classification No. CIO 2151.0. 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 2101.0. This document establishes Agency requirements that allow limited personal use of EPA managed resources.
- Interim Policy for Protecting PII, EPA Classification No. CIO-Tran. 6-11. This document establishes the requirements for protecting PII.
- Interim Procedures for Transmitting Sensitive Personally Identifiable Information (PII). This document establishes the requirements for transporting and/or transmitting PII.

8. ROLES AND RESPONSIBILITIES

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

Chief Technology Officer (CTO) and Director, Office of Technology Operations and Planning (OTOP) 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.

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 (excluding enterprise mobile devices).
- 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 with regard to the appropriate use and protection of all EPA managed mobile computing resources and information.
- 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.

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. RELATED PROCEDURES, STANDARDS AND GUIDANCE

- EPA Personal Property Policy and Procedures Manual. This 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 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 that are 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 Environmental Protection Agency (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.
- System Life Cycle Management Procedures, EPA Classification No. CIO 2121-P-03.0. This document establishes the EPA approach and practices in the pre-definition, definition, acquisition/development, implementation, operations and maintenance, and termination of EPA information technology (IT) systems and applications.
- Enterprise Architecture Procedures. These documents establish EPA's enterprise architecture requirements for EPA managed IT/IM solutions.
- Mobile Computing Management Procedures, EPA Classification No. CIO-2150.3-P-19.1. This document establishes the requirements for implementing and managing the use of government furnished information management and technology solutions.

12. MATERIAL SUPERSEDED

N/A

13. ADDITIONAL INFORMATION

For more information on this policy, 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