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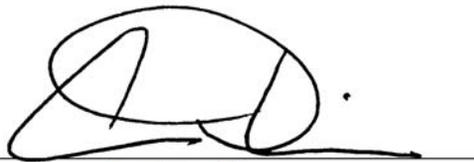
Ann Dunkin
Chief Information Officer
U.S. Environmental Protection Agency

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 Classification No.: CIO-2104.0-P-01.0	CIO Approval Date: 1/26/10
CIO Transmittal No.: 10-003	Review Date: 1/13

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-84, dated June 7, 2005

SOFTWARE MANAGEMENT AND PIRACY PROCEDURE

1   PURPOSE

The purpose of this procedure is to describe the process EPA Program Offices and Regions must follow to comply with the Environmental Protection Agency's (EPA or Agency) Software Management and Piracy Policy and Executive Order 13103, Computer Software Piracy. This Procedure is based on the Federal CIO (Chief Information Officer) Council's guidelines.

2   SCOPE AND APPLICABILITY

This Procedure is applicable to all EPA-approved software and the hardware using that software. It governs the actions and behaviors of anyone using or installing software on any EPA computer system, and using or installing any EPA-approved software.

3   AUDIENCE

All users of EPA-owned or leased computers, systems, and/or software; EPA contractors; and recipients of EPA federal financial assistance must adhere to this procedure.

4   BACKGROUND

Executive Order (EO) 13103 (September 30, 1998) on Computer Software Piracy states that each federal agency must develop a software management policy on the acquisition and use of software by the Agency and its employees. Compliance with EO 13103 establishes and ensures that the Agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws. In addition, effective software management helps to protect EPA information as a valuable national resource. EPA issued a Software Management and Piracy Policy to ensure that the Agency continues to meet the requirements of EO 13103.

To provide specific procedural information to managers and staff across EPA, the Office of Environmental Information (OEI) developed this Software Management and Piracy Procedure to accompany the updated Software Management and Piracy Policy, which replaces the policy issued in 2003.

5   AUTHORITY

EPA's Software Management and Piracy Policy , CIO 2104.1, 1/26/10

6   RELATED DOCUMENTS

- Agency Network Security Policy, CIO 2150.0, Nov. 27, 2007
http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2150-0.pdf

- Chief Information Officers (CIO) Council model policy on "Implementing the Executive Order on Computer Software Piracy" (June 2000)
http://www.cio.gov/NonSecure_Link/NonSecure_Link.cfm

- CIO 2101.0, EPA's Policy on Limited Personal Use of Government Office Equipment
http://intranet.epa.gov/oei/imitpolicy/qic/ciopolicy/2101-0.pdf

- EPA Delegation of Authority 1-84, Information Resources Management
http://intranet.epa.gov/rmpolicy/ads/dm/1-84_534.htm

- EPA LAN Operating Procedures (LOPS) Current Version
http://intranet.epa.gov/nis/lops.html
  - Chapter 1: Introduction
  - Chapter 2: Standard Hardware and Software
  - Chapter 3: Roles and Responsibilities
  - Chapter 4: LAN Server Applications
  - Chapter 5: LAN Workstation Applications
  - Chapter 7: Desktop Operation Systems
  - Chapter 10: LAN Security
  - Chapter 11: Remote Access

- EPA Order 3120.1, Conduct and Discipline Manual
http://intranet.epa.gov/rmpolicy/ads/orders/3120_1.pdf

- Executive Order 13103 on Computer Software Piracy
http://www.bsagovernment.com/downloads/guidelinesForImplimenting.pdf

- National Computer Center Operational Directives
http://basin.rtpnc.epa.gov/ntsd/directives.nsf/BySub?OpenView

- U.S. Office of Government Ethics, Standards of Ethical Conduct for Employees of the Executive Branch, U.S. Office of Government Ethics, October 2002
http://www.usoge.gov/ethics_docs/publications/reference_publications/rfsoc_02.pdf

7 SOFTWARE MANAGEMENT AND PIRACY PROCEDURE

Each Program Office or Region must establish auditable procedures to ensure that all software purchased or acquired and all software installed on EPA computer systems adheres to EPA's Software Management and Piracy Policy. This includes freeware, shareware and demonstration software.

To avoid purchasing or installing illegal software, each Information Management Officer must ensure that their Program Office or Region:

- Installs only software that is properly licensed and approved for use on EPA computer systems, including personal computers (PCs) and servers;

- Purchases software from reputable resellers: demands proper licenses and accompanying materials and validates licenses from these resellers;

- Documents and verifies appropriate licenses;

- Verifies that the licenses authorize EPA to distribute and use the software in the intended manner;

- Maintains a record-keeping system that tracks appropriate documentation for each software license including software name, version, vendor, number of licenses and the date of acquisition or license renewal, expiration date, and installation location;

IMOs are not responsible for enterprise (Agency) licenses, including core-configuration software (Lotus Notes, MS-Word, etc.). The Agency's Chief Technology Officer (CTO) and OEI's Office of Technology Operations and Planning are responsible for managing enterprise software licenses. OEI will provide training/awareness to end users on the requirements of the Software Management and Piracy Policy and Procedure in the required, annual Cybersecurity Awareness Training.

Agency software purchasers, managers, IT technicians and end users must be knowledgeable of applicable license requirements. Employees should report any violations of the Software Management and Piracy Policy to their Information Management Officer for appropriate investigation, enforcement or disciplinary action. Questions regarding license requirements should be directed to the official or manager who approved the software's installation. Questions regarding enterprise-wide licenses should be directed to the Office of Technology Operations and Planning. Any questions about copyright law should be directed to EPA's Office of General Counsel.

8 ROLES AND RESPONSIBILITIES

Chief Technology Officer (**CTO**) is responsible for providing procedures, standards, and guidance to senior level managers in support of the Agency's Software Management and Piracy Policy, for managing enterprise software licenses, and for providing covered users within their office with training/awareness on the Software Management and Piracy Policy through the annual Cybersecurity Awareness Training.

Senior Information Officials (SIOs) have primary responsibility for ensuring that their office is in compliance with the Software Management and Piracy Policy and Procedures.

Information Management Officers (IMOs) are responsible for:

- Establishing auditable procedures to ensure all software acquired and/or installed within or for their organization adheres to the Software Management and Piracy Policy.
- Ensuring the acquisition of all software includes appropriate EPA-acquired licenses, and use is in accordance with those licenses.
- Maintaining appropriate records or software licenses in an inventory tracking system.
- Ensuring that all their office's contracts and/or assistance agreements include provisions requiring the contractor or grantee to comply with this procedure.
- Approving software for purchase and use within their office.

This IMO responsibility does not apply to enterprise software licenses (see CTO role)

Information Security Officers (ISOs) are responsible for any security activities that pertain to software management and piracy.

IT Managers must ensure that the licensing and use of all software complies with the purchased licenses and establish any appropriate compensating controls to guard against software piracy in their Office.

Network administrators, system administrators and desktop technicians must:
- deploy only software and software upgrades with EPA-acquired licenses onto computer systems of their organizations; and
- monitor all systems to ensure that no unauthorized software is loaded.

End Users must install and use only software that has been appropriately acquired by EPA and is in compliance with the software vendor's license agreement. This includes Agency-purchased software, freeware, and shareware.

Office of Environmental Information, Office of Technology Operations and Planning, Enterprise Desktop Solutions Division (OEI-OTOP-EDSD) addresses questions and concerns regarding interpretation of these procedures.

9   DEFINITIONS

Software: Programs and applications that run on a computer, for example word processors, spreadsheets, and databases. This procedure is inclusive of all software applications including those that are original equipment manufacturer or 'bundled' software, freeware, shareware and demonstration software.

Personal Computer (PC): All Agency-owned or leased laptop and desktop computers.

Personally-owned Computer: Any laptop or desktop computer owned by the employee.

Piracy: Illegally copying software, using software that violates licensing restrictions, and/or other misuse of the license agreement.

10 WAIVERS

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

11 RELATED PROCEDURES AND GUIDELINES

N/A

12 MATERIAL SUPERSEDED

EPA's Guidelines for the Software Management and Piracy Policy, June 2003

13 ADDITIONAL INFORMATION

For more information on this procedure, please contact the Office of Environmental Information, Office of Technology Operations and Planning, Enterprise Desktop Solutions Division.

Linda A. Travers
Principal Deputy Assistant Administrator
Office of Environmental Information