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

OFFICE OF ENVIRONMENTAL INFORMATION

EPA Classification No.: CIO-2104.1	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 1-19, dated 07/07/2005

SOFTWARE MANAGEMENT AND PIRACY POLICY

1. PURPOSE

This Software Management and Piracy Policy establishes and describes the Environmental Protection Agency's (EPA or Agency) approach to complying with Executive Order 13103 (September 30, 1998) on Computer Software Piracy. The primary purpose of this policy is to ensure that all EPA-approved software is appropriately licensed, approved for use, and is not pirated software.

2. SCOPE AND APPLICABILITY

This policy covers 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 policy.

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 is issuing this policy, which replaces EPA's previous policy on Software Management and Piracy issued in May 2003, to ensure that the Agency continues to meet the requirements of EO 13103. Many of the details contained in the previous policy will be included in a separate Software Management and Piracy Procedure.

5. AUTHORITY

- Clinger-Cohen Act of 1996
http://www.ed.gov/policy/gen/leg/cca.html

- Copyright Act, Title 17 of United States Code.
http://www.law.cornell.edu/uscode/html/uscode17/usc_sup_01_17.html

- Digital Millennium Copyright Act of 1998
http://www.copyright.gov/legislation/dmca.pdf

- Executive Order 13103 (September 30, 1998) on Computer Software Piracy
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=1998_register&docid=fr05oc98-130.pdf

- Federal Acquisition Regulation, 48 C.F.R. Part 27, Patents, Data, and Copyrights
http://ecfr.gpoaccess.gov/cgi/t/text/text-idx?c=ecfr&tpl=/ecfrbrowse/Title48/48cfr27_main_02.tpl

- Federal Information Security Management Act of 2002, 44 U.S.C. 3541 et seq.
http://csrc.nist.gov/drivers/documents/FISMA-final.pdf

- OMB Circular A-130, Appendix III
http://www.whitehouse.gov/omb/circulars/a130/a130appendix_iii.html

6. POLICY

Only software that is properly licensed and approved for use may be installed on EPA computer systems, including personal computers (PCs) and servers. This requirement also applies to freeware, shareware and demonstration software. Any Agency-approved software installed on a personally-owned computer approved for flexiplace use must carry an appropriate Agency software license.

All software procured by the Agency is subject to the software publisher's license agreement. That agreement typically restricts how, and to whom, the software may be distributed. Agency software purchasers, IT technicians, end users, and anyone who approves the installation of software on Agency hardware must be knowledgeable of applicable license requirements and ensure that the use of the software will not violate any restrictions imposed by the software publisher.

EPA employees who purchase and install Agency software must do so in accordance with EO 13103 on Computer Software Piracy. Information Management Officers (IMOs), within each Program Office or Region, must ensure that software acquired by the Agency and approved for installation on Agency computers:

- has the appropriate license(s);
- is used in accordance with applicable licenses; and
- is appropriately documented with records of the software license(s).

Only software that has been approved by the IMO or the Agency's Chief Technology Officer and properly acquired by the Agency may be installed on EPA computer systems. IMOs are not responsible for enterprise (Agency) licenses, including core-configuration software (Lotus Notes, MS-Word, etc.). The Agency's CTO and OEI's Office of Technology Operations and Planning are responsible for managing enterprise software licenses.

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

The requirements of this Policy apply to existing as well as new or modified/enhanced software and software systems.

Consequences for Software Piracy or License Misuse

Please refer to the Standards of Ethical Conduct for Employees of the Executive Branch and to EPA Order 3120.1, Conduct and Discipline.

7. RELATED DOCUMENTS

- 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

- E-Government Act of 2002
http://www.whitehouse.gov/omb/egov/g-4-act.html

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

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

- EPA's Directive 2195 A1, EPA Information Security Manual
http://intranet.epa.gov/rmpolicy/ads/manuals/Manual.PDF

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

- 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

8. ROLES AND RESPONSIBILITIES

The **Chief Information Officer (CIO)**, who is also the Assistant Administrator for the Office of Environmental Information, is responsible for issuing the Software Management and Piracy Policy and providing Offices and Regions with guidance to help them comply with the requirements of this policy.

The **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 and for managing enterprise software licenses.

Senior Information Officials (SIOs) are responsible for ensuring compliance with the Software Management and Piracy Policy within their office, and for apprising the Quality and Information Council (QIC) of major Software Management and Piracy Policy issues within their office.

Information Management Officers (IMOs) are the approving authority for purchase and use of software within their office (excluding enterprise software) and are responsible for carrying out procedures that support compliance with the policy within their office.

Information Security Officers (ISOs) are responsible for ensuring that responsible program offices and individuals throughout their Program or Regional Office are cognizant of security requirements and processes mandated by this policy.

EPA Managers are responsible for addressing incidents of non-compliance with this policy. Managers may choose to inventory the software installed on an employee's computer system at any time.

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

EPA Employees, PC Administrators and Other Users must ensure that only software that is properly acquired and licensed by the Agency is installed on the Agency computer systems. Employees and other users must exercise common sense and good judgment in the use of government office equipment and government-approved software. Employees must safeguard, protect, and conserve government property and are responsible for the care, safety, and effective use of that property in accordance with this policy. Employees should report any misuse or unauthorized copying of software within the organization or Agency to his/her manager.

The Office of Environmental Information, Office of Technology Operations and Planning (OEI-OTOP) is responsible for addressing questions and concerns regarding software licensing and interpretation of this policy.

9. DEFINITIONS

For purposes of this policy:

Computer System: Any type of equipment that stores, processes, or transmits electronic data such as a server, desktop computer or laptops.

EPA Approved: The Agency holds an enterprise license to use the software or the local IMO has approved the software for purchase or use on an EPA computer system.

Software: Programs and applications that run on a computer, for example, word processors, spreadsheets and databases. This policy 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: Illegal duplication of software for commercial or personal use. For purposes of this policy, “piracy” will also mean use of software that violates licensing restrictions and/or other misuse of the license agreement.

Pirated Software

Types of pirated software or licensing violations include:

- Software that has been illegally copied
- Software that has been reproduced and/or distributed in violation of a software license

Examples of pirated software include:

- ***Counterfeit software:*** unauthorized copies of software created with the intent to directly imitate the copyrighted product. Counterfeit software is typically reproduced and distributed in a form to make the product appear legitimate and thus may include sophisticated efforts to replicate packaging, documentation, registration, logos, and security features.

- ***Compilation Compact Discs (CDs):*** unauthorized copies of multiple software programs compiled onto a single CD. Compilation CDs typically include software programs published by a variety of software publishers.

- ***Online pirated software:*** unauthorized copies of software distributed and downloaded via the Internet (including through peer-to-peer file sharing).

- ***Other illegally copied software:*** software copied from disks, CDs, or other machines without authorization of the copyright owner.

10. WAIVERS

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

11. RELATED PROCEDURES, STANDARDS AND GUIDANCE

- 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

12. MATERIAL SUPERSEDED

This policy supersedes CIO Policy 2104.0 (formerly EPA Order 2165.1, Software Management and Piracy Policy, dated May 2003).

13. ADDITIONAL INFORMATION

For more information on this policy, contact your Information Management Officer. You also may contact the Office of Environmental Information, Office of Technology Operations and Planning, Enterprise Desktop Solutions Division.

Linda A. Travers

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