



# ADMINISTRATIVE COMMUNICATIONS SYSTEM U.S. DEPARTMENT OF EDUCATION

## DEPARTMENTAL DIRECTIVE

OCIO: 3-110

Page 1 of 13 (03/10/2015) Original Date  
(12/06/2016) Re-certified Date

*Distribution:*  
All Department of Education  
Employees

*Signed by:* Andrew Jackson  
Assistant Secretary for Management

### Software Asset Management and Acquisition Policy

#### Table of Contents

Software Asset Management and Acquisition Policy .....	1
I. Purpose .....	2
II. Authorization .....	2
III. Applicability .....	2
Attachment A: Software Examples.....	8
Attachment B: Executive Order 13103.....	9

Supersedes ACS Handbook OCIO-08 "Handbook for Software Management and Acquisition Policy" dated 03/10/2015). Added Federal Source Code. Re-certified on 12/06/2016.

For technical questions regarding this ACS document, please contact John Faircloth via e-mail at [john.faircloth@ed.gov](mailto:john.faircloth@ed.gov)

## I. Purpose

The U.S. Department of Education (Department) is implementing this Software Asset Management and Acquisition Policy (SAMA Policy) to meet compliance standards, applicable laws, and licensing restrictions as outlined by Executive Order 13103, Computer Software Piracy. This SAMA Policy describes how the Department will comply with the Order and Implementation Guidelines issued by the Chief Information Officers Council (CIOC) and managed by the Office of the Chief Information Officer (OCIO).

## II. Authorization

- A. Executive Order 13103, titled Computer Software Piracy was signed by President Clinton on September 30, 1998 (see Attachment A). The Order can be found at 63.Fed.Reg.53273 (October 5, 1998).
- B. Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (OMB M-16-21, August 8 2016)

## III. Applicability

This Directive applies to all Department employees, all contractors utilizing Department-owned information technology equipment and software, and all information technology (IT) equipment that is connected to the Department's network (EDUCATE). This Directive supersedes ACS Handbook OCIO-08, Handbook for Software Asset Management and Acquisition Policy in describing the Department's procedures for software management and acquisition.

The Department's IT Security Compliance Guide (ITSCG) under Section 2.1 Governance paragraph two states, "For each system and application within the Principal Offices, the Information System Security Officers (ISSO) and Information System Officers (ISO) will assist in and monitor the implementation and effectiveness of the Department's IT security governance program." This includes the removal of unauthorized software.

The Secretary has formally endorsed the security goals outlined within the ITSCG and is responsible for the implementation of the Department's IT Security Program in accordance with the Federal Information Security Management Act (FISMA).

Executive Order 13103 Section 2 (a) states “Agency heads will ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency’s computers.”

#### **A. Removal of *Unauthorized Software***

The ED Security Operations Center (EDSOC) will monitor the network for unauthorized software and will notify the Enterprise Architecture Review Board (EARB) of any suspected unauthorized software. At which point the EARB will verify whether the software is/is not approved. After EARB verification of status, the IT POC will verify whether there is a license for the software. If there is no license agreement on record, the IT POC, in conjunction with the ISSO, will take appropriate action to remove any unlicensed software and provide impacted employees with timely notification that software was removed and stating the reason why. The impacted employee will be kept informed throughout the entire process, until the software is either removed or allowed to be kept on their machine.

#### **B. Software Management Review and Inventory**

OCIO Information Technology Program Services (ITPS) and the IT POCs will conduct an annual assessment of software management procedures, practices and an inventory of installed software and related license agreements, purchase invoices, and other documentation showing evidence of licensed software that is currently in use. OCIO ITPS and the IT POCs will use the software asset management (SAM) tool to retrieve reports to assist with enforcing and validating this SAMA Policy.

#### **C. Software Library**

For software that the Department or employees has legally obtained licensing and approval, OCIO, specifically ITPS, will maintain a software library for the Department for original software licenses, certificates of authenticity, purchase invoices, completed registration cards, original software media (e.g., diskettes or CD-ROMs), user, administrator, and assessment information. IT POCs will be required to enter all applicable information in the SAM tool, with OCIO ITPS acting as system administrator for the tool.

As part of the Department's Software Library an Open Source Software repository as defined in the Federal Source Code Policy: Achieving Efficiency, Transparency, and Innovation through Reusable and Open Source Software (OMB M-16-21, August 8, 2016).

All EARB approved software is available to Department employees for use (e.g., installation/re-installation, replacement, and upgrades) with approval from their IT POC or designee (providing licenses are available). Depending on the number of users for the software, the software will either be packaged or pushed to the users or a helpdesk technician will come to the user's desk to install the software. The software is the sole responsibility of helpdesk technicians while in their care.

#### **D. Software Use**

The following software policy applies to all Department employees and contractors who work at either a Department site or off-site (e.g. flexi-place and approved alternate work sites.)

*Prohibition against Unlicensed (and non-Department approved) Software Use.*

No employee or contractor will:

1. Install, reproduce, distribute, transmit, download, or otherwise use software for which the Department lacks the appropriate license, unless such software is properly licensed to the employee or contractor and is approved and used in accordance with Department policy and the applicable license. As part of IAS' continuous monitoring program, the EDSOC will be monitoring for unapproved/unauthorized software and weekly report will be generated and sent to the EARB for verification and validation. If the software is approved/authorized the user will be given access to the software. If the software is not approved/authorized, the software will be blacklisted. The user will make a request, written or verbal, to the IT POC who submits an EARB request to have the software approved.
2. Loan, distribute, or transmit Department software to any third party, unless the employee or contractor is expressly authorized to do so by OCIO and the applicable license.

#### **E. Authorization to Use Licensed Software on Department Owned Computers or Contracted Assets**

Authorization to use licensed software on Department-owned computers or contracted assets off-site (e.g., flexi-place and tele-centers): No employee or contractor will down install ANY software that has not been properly tested in

accordance with Department standards on Department computers unless otherwise directed to do so by written authorization from the CIO or his/her designated representative.

#### F. Enforcement

Any software for which OCIO or the IT POC does not have a license or is not approved will be enforced via the Continuous Monitoring program and blacklisted by the EDSOC, until approved. Users who do not have Admin Rights to their workstations and who inadvertently end up with unauthorized software are not liable but will still need to follow the approval process and meet license requirements, if the software is needed or required.

#### G. Responsibility

Employee/Contractor Responsibility – It is the employee and contractor's responsibility to ensure that no unlicensed software is installed on the agency computer.

- 1 **ISSO Responsibility** – It is the EDSOC's responsibility to report to the PO ISSO's and to the employee's supervisor the use of unlicensed software, and follow-up with the EDSOC helpdesk for software blacklisting. The contractor will notify their COR.
- 2 **Supervisor Responsibility** – It is the EDSOC's responsibility to ensure that unlicensed software is blacklisted from the employee and contractor's desktops once reported by the EDSOC. The supervisor will work with the user and the EARB to get the software approved, if needed.
- 3 **Helpdesk Technician Responsibility** – It is the helpdesk technician's responsibility to ensure that s/he does not install or assist in the installation of unlicensed software on the agency computer.
- 4 **EDSOC Responsibility** – It is the EDSOC's responsibility to continuously monitor the EDUCATE network for unlicensed/unapproved/unauthorized software and provide a weekly report to the EARB.

#### H. Education and Training

The Department will provide training to current and new employees on compliance with the Executive Order 13103 and this SAMA Policy. As part of such education and training, the Department will:

- 1 Provide training during employee orientation on SAMA Policy regarding the detection and prevention of piracy and the consequences of violating SAMA Policy and applicable copyright laws.
- 2 Circulate reminders of this SAMA Policy on a bi-annual basis. Reminders will be posted on connectED and SharePoint on a quarterly basis, along with specific email reminders directly to employees.
- 3 Review this policy annually as part of the required Department's Security Awareness Program.

#### **I. Performance Measures**

OCIO ITPS will develop performance measures to monitor the Department's compliance with the Executive Order 13103, CIOC, and this SAMA Policy on a quarterly basis.

EDSOC will run a weekly report of blacklisted/whitelisted software and provide a copy to the EARB for verification and validation. OCIO ITPS will run quarterly reports on software applications and provide a copy to the EDSOC and the EARB to ensure the Department is in compliance with this Directive.

#### **J. Unauthorized Software**

Unauthorized software includes pirated software or copyright infringement in the use of software. For purposes of this policy, pirated software or copyright infringement includes illegally copied and/or downloaded software that violates licensing restrictions. Illegally copied software or software infringement may include or be generated from: bundle software, compilation CDs, counterfeit software, hard-disk loaded software, or other illegally copied software.

#### **K. Shareware/Freeware/Open Source**

The use of copyrighted software or shareware and personally owned software is controlled and documented by the IT POC and the EARB. Use of Open source software is permitted, but the software MUST be assessed by the EARB to determine its security impact prior to use. Public domain software products (other than open source software products) may only be used in Department information systems if the product is assessed for security impacts and is explicitly approved for use by the EARB. Binary or machine executable public domain software products and other software products with limited or no warranty, such as those commonly known as freeware or shareware, are not permitted for use on agency computers unless approved

by the EARB as necessary for mission accomplishment without any known alternative solutions available. Project Managers are required to review the inventory of government-developed custom software available as Open Source Software at code.gov in accordance with the OMB M-16-21 Federal Source Code Policy.

**L. Browser Plugins and Extensions**

This policy does not apply to plug-ins or extensions, unless expressly prohibited by the CIO, EDSOC, or the EARB.

**M. Questions**

Employees with questions about this policy will address them to their supervisor, IT POC and the contractor should address questions to their Contracting Officer Representative. (COR) Employees can locate the contact information of their IT POC and ISSOs at the following link on connectED: <https://share.ed.gov/teams/OCIO/ITPS/PMT/SitePages/Home.aspx>

## Attachment A: Software Examples

### Open Source Software –

- Apache HTTP Server
- GIMP
- MySQL
- PERL

### Public Domain Software

- GameSWF – Flash video/game player
- SQLite
- HippoDraw

### Binary Machine Executable Public Domain Software

- BASIC
- MATLAB
- Python Freeware
- Skype
- Adobe Reader
- Free  
Studio

### Shareware

DVD-Clone VI

Registry Mechanic

Total Privacy

Wondershare YouTube Downloader



**Attachment B: Executive Order 13103****Presidential Documents****Executive Order 13103 of September 30, 1998****Computer Software Piracy**

The United States Government is the world's largest purchaser of computer-related services and equipment, purchasing more than \$20 billion annually. At a time when a critical component in discussions with our international trading partners concerns their efforts to combat piracy of computer software and other intellectual property, it is incumbent on the United States to ensure that its own practices as a purchaser and user of computer software are beyond reproach. Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1. Policy.** It shall be the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of Federal law, including the Copyright Act.

(a) Each agency shall adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.

(b) Each agency shall establish procedures to ensure that the agency has present on its computers and uses only computer software not in violation of applicable copyright laws. These procedures may include:

- (1) preparing agency inventories of the software present on its computers;
- (2) determining what computer software the agency has the authorization to use; and
- (3) developing and maintaining adequate recordkeeping systems.

(c) Contractors and recipients of Federal financial assistance, including recipients of grants and loan guarantee assistance, should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. If agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors or recipients may affect the integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law.

(d) Executive agencies shall cooperate fully in implementing this order and shall share information as appropriate that may be useful in combating the use of computer software in violation of applicable copyright laws.

**Sec. 2. Responsibilities of Agency Heads.** In connection with the acquisition and use of computer software, the head of each executive agency shall:

- (a) ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency's computers;

(b) utilize performance measures as recommended by the Chief Information Officers Council pursuant to section 3 of this order to assess the agency's compliance with this order;

(c) educate appropriate agency personnel regarding copyrights protecting computer software and the policies and procedures adopted by the agency to honor them; and

(d) ensure that the policies, procedures, and practices of the agency related to copyrights protecting computer software are adequate and fully implement the policies set forth in this order.

**Sec. 3. Chief Information Officers Council.** The Chief Information Officers Council ("Council") established by section 3 of Executive Order No. 13011 of July 16, 1996, shall be the principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software. The Council shall provide advice and make recommendations to executive agencies and to the Office of Management and Budget regarding appropriate government-wide measures to carry out this order. The Council shall issue its initial recommendations within 6 months of the date of this order.

**Sec. 4. Office of Management and Budget.** The Director of the Office of Management and Budget, in carrying out responsibilities under the Clinger-Cohen Act, shall utilize appropriate oversight mechanisms to foster agency compliance with the policies set forth in this order. In carrying out these responsibilities, the Director shall consider any recommendations made by the Council under section 3 of this order regarding practices and policies to be instituted on a government-wide basis to carry out this order.

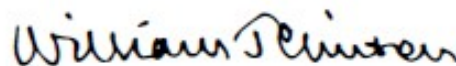
**Sec. 5. Definition.** "Executive agency" and "agency" have the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

**Sec. 6. National Security.** In the interest of national security, nothing in this order shall be construed to require the disclosure of intelligence sources or methods or to otherwise impair the authority of those agencies listed at 50 U.S.C. 401a(4) to carry out intelligence activities.

**Sec. 7. Law Enforcement Activities.** Nothing in this order shall be construed to require the disclosure of law enforcement investigative sources or methods or to prohibit or otherwise impair any lawful investigative or protective activity undertaken for or by any officer, agent, or employee of the United States or any person acting pursuant to a contract or other agreement with such entities.

**Sec. 8. Scope.** Nothing in this order shall be construed to limit or otherwise affect the interpretation, application, or operation of 28 U.S.C. 1498.

**Sec. 9. Judicial Review.** This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.



THE WHITE HOUSE,  
September 30, 1998.

Executive Order 13103 of September 30, 1998

### Computer Software Piracy

The United States Government is the world's largest purchaser of computer-related services and equipment, purchasing more than \$20 billion annually. At a time when a critical component in discussions with our international trading partners concerns their efforts to combat piracy of computer software and other intellectual property, it is incumbent on the United States to ensure that its own practices as a purchaser and user of computer software are beyond reproach. Accordingly, by the authority vested in me as President by the Constitution and the laws of the United States of America, it is hereby ordered as follows:

**Section 1.** Policy. It shall be the policy of the United States Government that each executive agency shall work diligently to prevent and combat computer software piracy in order to give effect to copyrights associated with computer software by observing the relevant provisions of international agreements in effect in the United States, including applicable provisions of the World Trade Organization Agreement on Trade-Related Aspects of Intellectual Property Rights, the Berne Convention for the Protection of Literary and Artistic Works, and relevant provisions of Federal law, including the Copyright Act.

- (a) Each agency shall adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws.
- (b) Each agency shall establish procedures to ensure that the agency has present on its computers and uses only computer software not in violation of applicable copyright laws. These procedures may include:
  - (1) preparing agency inventories of the software present on its computers;
  - (2) determining what computer software the agency has the authorization to use; and
  - (3) developing and maintaining adequate recordkeeping systems.
- (c) Contractors and recipients of Federal financial assistance, including recipients of grants and loan guarantee assistance, should have appropriate systems and controls in place to ensure that Federal funds are not used to acquire, operate, or maintain computer software in violation of applicable copyright laws. If agencies become aware that contractors or recipients are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determine that such actions of the contractors

or recipients may affect the integrity of the agency's contracting and Federal financial assistance processes, agencies shall take such measures, including the use of certifications or written assurances, as the agency head deems appropriate and consistent with the requirements of law.

- (d) Executive agencies shall cooperate fully in implementing this order and shall share information as appropriate that may be useful in combating the use of computer software in violation of applicable copyright laws.

**Sec. 2. Responsibilities of Agency Heads.** In connection with the acquisition and use of computer software, the head of each executive agency shall:

- (a) Ensure agency compliance with copyright laws protecting computer software and with the provisions of this order to ensure that only authorized computer software is acquired for and used on the agency's computers;
- (b) Utilize performance measures as recommended by the Chief Information Officers Council pursuant to section 3 of this order to assess the agency's compliance with this order;
- (c) Educate appropriate agency personnel regarding copyrights protecting computer software and the policies and procedures adopted by the agency to honor them; and
- (d) Ensure that the policies, procedures, and practices of the agency related to copyrights protecting computer software are adequate and fully implement the policies set forth in this order.

**Sec. 3. Chief Information Officers Council.** The Chief Information Officers Council ("Council") established by section 3 of Executive Order No. 13011 of July 16, 1996, shall be the principal interagency forum to improve executive agency practices regarding the acquisition and use of computer software, and monitoring and combating the use of unauthorized computer software. The Council shall provide advice and make recommendations to executive agencies and to the Office of Management and Budget regarding appropriate government-wide measures to carry out this order. The Council shall issue its initial recommendations within 6 months of the date of this order.

**Sec. 4. Office of Management and Budget.** The Director of the Office of Management and Budget, in carrying out responsibilities under the Clinger-Cohen Act, shall utilize appropriate oversight mechanisms to foster agency compliance with the policies set forth in this order. In carrying out these responsibilities, the Director shall

consider any recommendations made by the Council under section 3 of this order regarding practices and policies to be instituted on a government-wide basis to carry out this order.

**Sec. 5.** Definition. “Executive agency” and “agency” have the meaning given to that term in section 4(1) of the Office of Federal Procurement Policy Act (41 U.S.C. 403(1)).

**Sec. 6.** National Security. In the interest of national security, nothing in this order shall be construed to require the disclosure of intelligence sources or methods or to otherwise impair the authority of those agencies listed at 50 U.S. 401a(4) to carry out intelligence activities.

**Sec. 7.** Law Enforcement Activities. Nothing in this order shall be construed to require the disclosure of law enforcement investigative sources or methods or to prohibit or otherwise impair any lawful investigative or protective activity undertaken for or by any officer, agent, or employee of the United States or any person acting pursuant to a contract or other agreement with such entities.

**Sec. 8.** Scope. Nothing in this order shall be construed to limit or otherwise affect the interpretation, application, or operation of 28 U.S.C. 1498.

**Sec. 9.** Judicial Review. This Executive order is intended only to improve the internal management of the executive branch and does not create any right or benefit, substantive or procedural, at law or equity by a party against the United States, its agencies or instrumentalities, its officers or employees, or any other person.

Signed: William J. Clinton

THE WHITE HOUSE

September 30, 1998