**DOE G 205.2-1**

Approved: 7-12-01

# GUIDE TO PREVENTING COMPUTER SOFTWARE PIRACY

*[This Guide describes suggested nonmandatory approaches for meeting requirements. Guides are not requirements documents and are not construed as requirements in any audit.]*



## U.S. DEPARTMENT OF ENERGY

## Office of the Chief Information Officer

**DISTRIBUTION:**
**All Departmental Elements**

**INITIATED BY:**
**Office of the Chief Information Officer**

**This page intentionally left blank.**

**CONTENTS**

**This page intentionally left blank.**

## 1.0 INTRODUCTION

President Clinton issued Executive Order 13103, Computer Software Piracy, on September 30, 1998. The Order states that "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." Computer software, secured by Federal copyright laws, protects the owner by requiring that users of a particular software program be issued a license for such use. The U.S. Government—the nation's largest consumer of software—has an essential role to play in establishing procedures to ensure that each agency has present on its computers and uses only computer software not in violation of applicable copyright laws. In providing guidance to Federal agencies on fulfilling this role, the Federal Chief Information Officers (CIO) Council issued recommendations regarding appropriate governmentwide measures to carry out the Executive Order's requirements. It is the intent of the Department of Energy (DOE) to issue guidance in accordance with Federal CIO Council recommendations and in compliance with Executive Order 13103. The guidance in this document is based on the CIO Council's recommendations in reference to computer software piracy, and applies to all DOE elements.

### 1.1 Federal Copyright Law[1]

The rights granted to the owner of a copyright are described in the Copyright Act, Title 17 of the United States Code (U.S.C.). The Act gives the owner of the copyright "the exclusive rights" to "reproduce the copyrighted work" and "to distribute copies . . . of the copyrighted work." It also states that "anyone who violates any of the exclusive rights of the copyright owner . . . is an infringer of the copyright" and sets forth penalties for such conduct.

Those who purchase a license for a copy of software do not have the right to make additional copies without the permission of the copyright owner except to (1) copy the software for use on a single computer and (2) make "another copy for archival purposes only." These rights are specifically provided in the Copyright Act; however, the license accompanying the product may allow additional copies to be made.

Unauthorized duplication of software constitutes copyright infringement regardless of whether it is done for sale, free distribution, or the copier's own use. Moreover, copiers are liable for the resulting copyright infringement whether or not they knew their conduct violated Federal law. Penalties include liability for damages suffered by the copyright owner plus any profits of the infringer that are attributable to the copying, or statutory damages of up to $100,000 for each work infringed upon. The unauthorized duplication of software is also a Federal crime if done "willfully and for purposes of commercial advantage or private financial gain (Title 18 Section 2319(b))." Criminal penalties include fines of as much as $250,000 and jail terms of up to 5 years.



---

[1] A glossary of copyright terms is provided in Appendix A.

## 1.2 Description of Executive Order 13103, Computer Software Piracy[2]

Executive Order 13103 sets forth the Government's policy against the use, acquisition, reproduction, distribution, and transmission of computer software that violates applicable copyright laws. To implement this policy, the Executive Order directs each executive agency to—

- adopt procedures to ensure that the agency does not acquire, reproduce, distribute, or transmit computer software in violation of applicable copyright laws;

- establish procedures to ensure that the agency has present on its computers and uses only computer software that does not violate applicable copyright laws. These procedures may include (1) preparing agency inventories of the software present on its computers; (2) establishing agency computer software authorization; and (3) developing and maintaining adequate record-keeping systems;

- take appropriate measures, including, for example, the use of certifications or written assurances, in the event the agency becomes aware that contractors or recipients of Federal financial assistance are using Federal funds to acquire, operate, or maintain computer software in violation of copyright laws and determines that such actions may affect the integrity of the agency's contracting and Federal financial assistance processes;

- cooperate fully in implementing the Executive Order and share information that may be useful in combating the use of computer software in violation of applicable copyright laws;

- educate appropriate agency personnel regarding software copyrights and the policies and procedures adopted by the agency to honor them; and

- 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 the Executive Order.



The Executive Order also directs the Office of Management and Budget to use its oversight mechanisms to foster compliance with the order.

## 1.3 The Office of the CIO Recommendations for Departmental Elements

The Office of the CIO recommends that Departmental elements develop and implement software management policies on the acquisition and use of software by its Federal and contractor staff. Such policies should—

---

[2] A copy of the Executive Order 13103 is provided in Appendix B.

- prohibit the use or installation of software for which appropriate licenses are nonexistent;
- guard against the acquisition of counterfeit software or software that violates licensing restrictions;
- adopt formal software installation and distribution procedures;
- establish procedures governing the use of user-owned software on Federal computers and the use of Federal software on home or remote computers that comply with applicable licenses;
- develop and implement procedures for monitoring compliance with software management policies;
- establish and maintain a record-keeping system for documentation and materials evidencing legal use of software; and
- develop a program for training new and existing staff on software management policies.

The Federal CIO Council has issued sample software management and acquisition policies, as well as recommended procedures for assessing compliance with these policies. Guidance is provided here to help Departmental elements develop appropriate policies and implement procedures to ensure compliance with the Executive Order and Federal copyright law. Sample Software Management Policy is provided in Section 2.0. Sample Software Acquisition Policy is provided in Section 3.0.

Sample templates to use when assessing compliance with these policies are provided in Section 4.0. Four templates are provided for—

- conducting a baseline assessment for software use (Part A);
- assessing software acquisition procedures (Part B);
- assessing software installation and management procedures (Part C); and
- assessing procedures for the management of original software and backup copies (Part D).

Finally, a sample software user survey is provided in Section 5.0 to help assess employees' use of software at the office and at home (for work performed at home).

### 1.4 The Most Common Types of Software Piracy[3]

The creation and/or installation of unauthorized copies of software is referred to as software piracy. The most common types of software piracy include counterfeiting, end-user piracy, compilation CD-ROMs, hard disk loading, client/server piracy, and online piracy.

**Counterfeiting.** Counterfeit software is an unauthorized copy of software that is duplicated with the intent of directly imitating the copyrighted product. Counterfeit software typically is 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.

**End User Piracy.** End user piracy occurs when organizations or individuals make unauthorized copies of software by (1) using one disk to install a program on multiple computers; (2) copying disks for installation and distribution; and (3) taking advantage of upgrade offers without having a legal copy of the version to be upgraded.

**Compilation CD-ROMs.** A compilation CD-ROM is a compact disc (CD) on which pirates have placed unauthorized copies of multiple software programs. Compilation CDs typically include software programs published by a variety of software publishers.

**Hard Disk Loading.** Hard disk loading occurs when unauthorized copies of software are loaded by the hardware dealer onto the hard disk of the computer and then offered to the customer as a free or heavily discounted incentive to purchase the computer.

**Client/Server Piracy.** Client/server piracy occurs when pirated copies of software are loaded onto an organization's servers for use in a network environment, or legitimate software is used outside the license terms (e.g., more simultaneous instances in use than allowed by the license).

**Online Piracy.** Online piracy occurs when unauthorized copies of software are distributed and downloaded using the Internet.



## 2.0 SAMPLE SOFTWARE MANAGEMENT POLICY

Paragraphs 1 through 8 of this section comprise a sample software management policy based on recommendations issued by the Federal CIO Council.

---

[3] Additional information on software piracy and misuse of software licenses is provided in Section 3.0, Sample Software Acquisition Policy.

1. **Purpose.** This Software Management Policy (Policy) sets forth steps the Departmental element must take to comply with Executive Order 13103, Computer Software Piracy.

2. **Software Acquisition and Installation Procedures.**

   - Where possible, all requests for software and software upgrades must be submitted to the Federal manager for information management (IM) or his/her designee.

   - All software and software upgrades not acquired by the IM manager must be documented and identified to the IM manager or his/her designee, who will verify that the Departmental element has an appropriate license for the use of such software.

   - All acquisitions of hardware that include bundled software must be documented and identified to the IM manager or his/her designee, who will verify that the Departmental element has an appropriate license for the use of such bundled software.

3. **Destruction of Unauthorized Software.** The IM manager or designated employees must destroy all copies of software for which the Departmental element lacks the appropriate license. Alternatively, the IM manager may obtain the license(s) necessary to maintain such software on Federal computers.

4. **Software Management Review and Inventory.** Periodically, the Departmental element must conduct—

   - an assessment of its software management procedures and practices and

   - an inventory of installed software and related license agreements, purchase invoices, and other proof of licensed software use.

5. **Record Keeping.** The Departmental element, under the supervision of the IM manager, must establish and maintain a record-keeping system for original software licenses, certificates of authenticity, purchase invoices, completed registration cards, original software media (e.g., diskettes, CD-ROMs, or mainframe computer tapes), user information, and assessment information. The Departmental element must maintain such information in a secure location(s) to minimize the risk of software theft and unauthorized duplication of software. The Department element also must consider the use of software management computer programs to automate such record keeping.

6. **Software Use Policy.** Employees should comply with the following software use policy:

   - Prohibition Against Unlicensed Software Use. Employees must not—

a. Install, reproduce, distribute, transmit, or otherwise use software for which this Departmental element lacks the appropriate license, unless such software is properly licensed to the employee and used in accordance with existing policy and the applicable license. If an employee becomes aware of the reproduction, distribution, or use of unauthorized software within this Departmental element, he/she should promptly notify his/her supervisor or the IM manager.

b. Install, reproduce, or use any software upgrade on a computer that does not already have resident on it the original version of the software.

c. Lend, distribute, or transmit Federal software to any third party, unless the employee is expressly authorized to do so by his/her supervisor and the applicable license.

- Authorization to Use Agency Software on Home Computers. The licenses for some Federal software permit employees of the Departmental element to make a copy of the software for home use. In such event, employees may make a copy of such software for home use only if they demonstrate a need to conduct Federal business from their homes and receive express authorization from their supervisor, the IM manager, or his/her designee. Under no circumstances, however, may an employee use Federal software for purposes other than DOE business.

- Downloading of Software from the Internet or Other Sources onto Federal Computers. A variety of software is available on the Internet. Some of this software, called "freeware" or "shareware," is available free of charge for limited uses and may be downloaded by an employee. (*NOTE: Depending on the Internet usage and security-related policies in effect within your Departmental element, supervisory approval may be required to permit employees to download work-related "freeware" and "shareware" from the Internet.*)

  Other software available on the Internet and from other electronic sources, however, requires the user to obtain a license for its use, sometimes for a fee. Employees must not download licensed software to their workstations without the prior approval of their supervisors, the IM manager, or his/her designee.

- Enforcement. The IM manager must supervise periodic reviews and assessments to evaluate the effectiveness of the software management policy.

- Accountability. An employee may be held responsible for the existence of any software on his/her workstation for which the Departmental element lacks the appropriate licenses.

- Questions. An employee may direct any questions concerning this Policy to his/her supervisor or the IM manager *[provide phone numbers, office locations, and e-mail addresses]*.

7. **Education and Training.** The Departmental element must provide education and training to all employees on (1) compliance with the Software Management Policy, (2) how to detect and prevent piracy, and (3) the consequences of violating the Software Management Policy and applicable copyright laws. The Departmental element must inform employees where they can get additional information on the Policy and software piracy prevention.

8. **Performance Measures.** The IM manager must develop performance measures to monitor compliance with the Software Management Policy. Examples of performance measures include (1) the number of software inventories conducted within the past 2 years; (2) the percentage of hardware assets included in the last inventory; (3) the number of software license violations detected in the last inventory; (4) license compliance; and (5) the percentage of employees who are aware of and understand the organization's software usage policies.

## 3.0 SAMPLE SOFTWARE ACQUISITION POLICY

Paragraphs 1 through 6 of this section comprise a sample software acquisition policy based on recommendations issued by the Federal CIO Council.

1. **Purpose.** This Software Acquisition Policy (Policy) was adopted to implement those provisions of Executive Order 13103, Computer Software Piracy, that require Federal agencies to acquire computer software in compliance with applicable laws and licensing restrictions. This Policy identifies categories of software that violate such laws or licensing restrictions and sets forth steps the Departmental element should take to avoid acquisition of illegal software. In addition, the Policy indicates remedial actions that should be taken in the event a software reseller supplies computer software that violates applicable laws or licensing restrictions.

2. **Types of Pirated Software.** To comply with Executive Order 13103, applicable laws, and licensing restrictions, the Departmental element and its employees should be cognizant of the different types of pirated software when evaluating bids or engaging in negotiations to acquire computer software. For purposes of this Policy, pirated software includes both illegally copied software and software that violates licensing restrictions.

   a. Illegally Copied Software. Illegally copied software includes counterfeit software, compilation CDs, hard-disk loaded software, online pirated software, and other illegally copied software.

      - Counterfeit Software. Unauthorized copies of software that are duplicated with the intent of directly imitating 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 CDs. Unauthorized copies of multiple software programs that are compiled onto a single CD. Compilation CDs typically include software programs published by a variety of software publishers.

- Hard-Disk Loaded Software. Unauthorized copies of software loaded by the hardware dealer onto the hard disk of the computer and then offered to the customer as a free or heavily discounted incentive to purchase the computer.

- Online Pirated Software. Unauthorized copies of software that are distributed and downloaded using the Internet.

- Other Illegally Copied Software. Software that is copied from disks, CDs, client/servers, or other machines without the authorization of the copyright owner.

b. License Misuse. Software copies are licensed, not sold, to the end user. The software publisher's license agreement typically restricts how, and to whom, software copies may be distributed. When acquiring software copies, the Departmental element should review the applicable license and ensure that its use of the software will not violate any restrictions imposed by the software publisher. License misuse occurs when legitimate copies of software are distributed and used in violation of the applicable license agreement. Examples of license misuse include the following:

- Original Equipment Manufacturer (OEM) Software. OEM software is licensed and specifically marked for distribution with new computer hardware. License misuse occurs when OEM software is "unbundled" from the computer and distributed to, and used by, the end user as a stand-alone product, often at a heavily discounted price.

- Academic Versions. Academic software is manufactured, licensed, and specifically marked for distribution to educational institutions and students at reduced prices. License misuse occurs when academic software is distributed to, and used by, a nonacademic end user.

- Not for Resale (NFR) Software. NFR software is marked "not for resale" and typically is distributed as promotional or sample product and not licensed for commercial distribution and use. License misuse occurs when NFR software is distributed in violation of its resale restrictions.

- Fulfillment Software. Fulfillment software is licensed solely for distribution to mid- or large-sized end users that possess a volume license agreement or valid site license. Fulfillment software is typically distributed in a CD jewel case without the packaging or materials that accompany a retail product. The fulfillment media is not itself a licensed product. License misuse occurs when fulfillment software is distributed to, and used by, end users that lack the necessary licenses for use of the underlying product. A similar situation occurs when a software license is used for purposes other than software development.

- Software Upgrades. Upgrade versions of software programs are licensed and specifically marked for distribution to end users that currently possess a valid license for the original product or a designated set of competitive products. License misuse occurs when upgrades are distributed to, and used by, end users that lack a license for the original product.

Typically, OEM, fulfillment, and other nonretail products are distributed without the colorful packaging and materials that accompany full retail products. Accordingly, these nonretail products are easier to counterfeit. Thus, Federal employees should be aware that deeply discounted nonretail software may, in fact, be counterfeit.

3. **Operational Defects of Pirated Software.** The Departmental element and its employees should be cognizant of the risks that accompany the acquisition and use of software in violation of applicable copyrights or licensing restrictions. Beyond the legal risks that accompany copyright and licensing violations, the use of pirated software can jeopardize the effectiveness and integrity of the Federal computer system. Pirated software typically lacks the full package of benefits that accompany a legitimate product, including the following:

   - warranty protection;
   - notice of, and ability to obtain, upgrades and repairs/fixes to the software;
   - technical support for the software;
   - assurances that the software is free of computer viruses and other malicious code; and
   - confidence that the most recent version of the software, free from defects, is being obtained.

4. **Steps to Avoid Acquisition of Pirated Computer Software.** The Departmental element and any employees authorized to acquire software should take all necessary steps to minimize the risk of acquiring pirated software, including the following:

   - Educate Employees. Employees authorized to acquire software should be educated on the requirements of Executive Order 13103 and this Software Acquisition Policy.
   - Standardize Software Acquisition Procedures and Centralize Purchases. The Departmental element should, to the extent possible:
     – implement standardized software acquisition procedures;
     – centralize software purchases within a designated department or group of employees who have been educated on the requirements of the Executive Order 13103 and this Software Acquisition Policy. By implementing standardized acquisition procedures and centralizing software purchases, the

Departmental element will be better able to prevent acquisition of pirated software. Moreover, a centralized acquisition program can result in volume purchases, which are often accompanied by discounts.

- Demand Proper Licenses and Accompanying Materials. Before purchasing software, the employee should research the license and materials that accompany the legitimate product (e.g., an original license agreement, registration card, manual, security features, and diskettes or CD-ROM). Federal employees should demand and obtain each of these materials and avoid software resellers that refuse to comply.

- Verify Appropriate License. Before purchasing software, verify that the license authorizes distribution to, and use by, the Departmental element.

- Purchase Software from Reputable Resellers. Employees should seek out software resellers with reputations for honesty and customer service within the community.

- Contact the Software Publisher. Particularly for large purchases of software, employees should contact the software publisher or its authorized distributor for information on the product and authorized resellers within the community. Moreover, the software publisher or authorized distributor should be contacted whenever an employee suspects that software acquired by, or offered to, the Departmental element may be pirated.

5. **Warning Signs of Pirated Software.** The Departmental element and any employees authorized to acquire software should be aware of the following "warning signs" that often accompany pirated software.

   - The price of the software is significantly below the software publisher's suggested retail price or otherwise appears "too good to be true."

   - The software is distributed in a CD jewel case without the packaging and materials that typically accompany a legitimate product.

   - The software lacks the software publisher's standard security features, such as a hardware lock or certificates of authenticity.

   - The software lacks an original license or other information from which the agency can verify that its use of such software is validly licensed by the copyright holder.

   - The packaging or materials that accompany the software have been copied or are of inferior print quality.

   - The CD contains software from more than one software publisher or programs that are not typically sold as a "suite."

   - The software is downloaded from the Internet without the software publisher's authorization.

- The software is distributed by a mail order or online reseller that fails to provide appropriate guarantees of legitimate product.

- The software contains markings indicating that distribution to, and use by, the Departmental element would violate the software publisher's license (e.g., "distribute only with new PC hardware," "Academic Version," "Upgrade," etc.).

- The software is loaded onto computer hardware without a separate license or invoice indicating a legitimate purchase.

6. **Steps to Take if Pirated Software is Suspected.** If an employee suspects that software offered or supplied by a reseller is pirated, he/she should contact the software publisher or an authorized reseller to investigate. If the employee's suspicions are confirmed, the Departmental element should take one or more of the following remedial actions.

   - Return the pirated software and request legitimate replacement software or a refund.

   - Withhold payment under the software contract until legitimate software is supplied.

   - Terminate the contract for failure to comply with its terms.

   - Suspend and/or debar the reseller for committing an offense that indicates a lack of business integrity, for engagement in fraud, or for willfully failing to comply with contract terms (debarment only). (See Federal Acquisition Regulation Subpart 9.4.)

   - Bring a False Claims Act action against the contractor for payments related to the illegal computer software.



## 4.0 SAMPLE TEMPLATES FOR ASSESSING COMPLIANCE WITH SOFTWARE MANAGEMENT AND ACQUISITION POLICIES

This section includes four sample templates that you may use when assessing compliance with software management and acquisition policies at your Departmental location. The first template identifies the steps necessary to conduct a baseline assessment of employees' software use (Part A). The second template identifies the questions to be asked when assessing software acquisition procedures (Part B). The third template identifies the questions to be asked when assessing software installation and management procedures (Part C). The final template identifies the questions to be asked when assessing procedures for the management of original software and backup copies (Part D).

**Part A. Conducting the Baseline Assessment of Software Use.**

| Pre-Assessment Procedures | | Date Completed |
|---|---|---|
| A.1. | Collect and review software purchase records. | |
| A.2. | Collect and review software licenses. | |
| A.3. | Determine whether to notify employees of assessment and distribute assessment information letter to employees, if warranted. | |
| A.4. | Determine whether to use software to perform certain functions of the initial assessment and select software package and vendor, if warranted. | |
| **Assessment Procedures** | | **Date Completed** |
| A.5. | Identify the location of servers, workstations, and all other hardware that run software programs. | |
| A.6. | Identify software resident. | |
| A.7. | Record the title, version, publisher, and serial number of software. | |
| A.8. | Record files not recognized by automated assessment programs or the inspector and determine whether such files are legitimate. | |
| A.9. | Estimate extent of home use of agency software by compiling results of the Software User Survey. | |
| A.10. | Match the record of software against licenses and ownership documentation to establish proof of authorization. | |
| A.11. | Reconcile number of users of software loaded on networks with the number of users accounted for in licenses. | |
| **Post-Assessment Procedures** | | **Date Completed** |
| A.12. | Delete and destroy unauthorized copies of software or obtain licenses for them. | |
| A.13. | Identify problem areas, if any, where the agency may focus training and educational efforts to reduce the use of unauthorized software. | |
| A.14. | Record results of the assessment. | |
| **Name/Title of Individual Completing Assessment:** | | |

**Part B. Assessing Software Acquisition Procedures.**

| | | Yes | No | Comments |
|---|---|---|---|---|
| B.1. | Does the Departmental element include software as a separate line item in its budgeting process? | | | |
| B.2. | Does the Departmental element purchase software through a central office? | | | |
| B.3. | Does the Departmental element obtain a sufficient number of licenses to cover the expected number of users? | | | |
| B.4. | Does the IM manager or other responsible official periodically review software licenses and ensure the agency's compliance with them? | | | |
| B.5. | Does the Departmental element ensure that it receives all required components (end user license agreement, registration card, manual, and CD) and security features for all retail or OEM software it acquires? | | | |
| B.6. | Does the Departmental element properly register purchased software? | | | |
| B.7. | Does the Departmental element maintain software registration and license information in a centrally located file and/or software management system? | | | |
| B.8. | If a software upgrade is requested or needed, does the Departmental element obtain the necessary updated licenses? | | | |
| B.9. | Does the Departmental element maintain a log listing the hardware and software at each workstation and each office location? | | | |
| B.10. | Does the Departmental element ensure that users have access to manuals and reference materials? | | | |
| B.11. | Does the Departmental element remove from its hard drives discontinued or obsolete software? | | | |
| **Date Assessment Completed:** | | | | |
| **Name/Title of Person Completing Assessment:** | | | | |

**Part C. Assessing Software Installation and Management Procedures.**

| | | | | |
|---|---|---|---|---|
| | | | | **Comments** |
| C.1. | What, if any, software is installed by the vendor? | | | |
| C.2. | What software is installed by Federal personnel? | | | |
| C.3. | Who authorizes installation of new software? | | | |
| C.4. | Who monitors installations? | | | |
| | | **Yes** | **No** | **Comments** |
| C.5. | Does the Departmental element use passwords or other methods to restrict access to particular software programs? | | | |
| C.6. | Are employees authorized to use agency-owned software at home for personal use? | | | |
| C.7. | Are employees authorized to use agency-owned software at home for agency business? | | | |
| C.8. | If so, does the Departmental element ensure that the applicable license agreement permits home use of agency-owned software? | | | |
| C.9. | Does the Departmental element permit employees to install personal software on their computers at work? | | | |
| C.10. | If so, does the Departmental element ensure that these programs are used in accordance with applicable license agreements? | | | |
| C.11. | Does the Departmental element review and document the software installed and used on each work station at regular intervals? | | | |
| C.12. | Are license agreements retained and filed with software serial numbers noted on hard copies? | | | |
| C.13. | Does the Departmental element reconcile its base of installed software with its software licenses at regular intervals? | | | |
| **Date Assessment Completed:** | | | | |
| **Name/Title of Person Completing Assessment:** | | | | |

**Part D. Assessing Procedures for the Management of Original Software and Backup Copies.**

| | | Yes | No | Comments |
|---|---|---|---|---|
| D.1. | Does the Departmental element make backup copies of original software? | | | |
| D.2. | Are original software diskettes/CD-ROMs and backup copies stored at a central location? | | | |
| D.3. | Does the Departmental element monitor the use and return of backup diskettes/CD-ROMs? | | | |
| D.5. | Does the Departmental element store original diskettes/CD-ROMs in a secure location where access is limited to authorized employees? | | | |
| D.6. | Who is responsible for making and storing backed up software? | | | |
| **Date Assessment Completed:** | | | | |
| **Name/Title of Person Completing Assessment:** | | | | |

## 5.0 SAMPLE SOFTWARE USER SURVEY

1. Which five software applications do you use most often at work and how frequently do you use them?

| | Software Application | Hours/Day |
|---|---|---|
| 1. | | |
| 2. | | |
| 3. | | |
| 4. | | |
| 5. | | |

2. Does your employer provide you with the software you need to perform your job tasks?

Yes _____ No _____

3. How did you obtain the software applications identified in Question 1? Check any of the following answers that apply.

_____ I access software through a centralized server.
_____ I obtained software from my supervisor.
_____ I obtained software from IT support personnel.
_____ I acquired software directly from a reseller.
_____ I downloaded software from the Internet.
_____ I copied software from another employee.
_____ I copied software from my home computer.
_____ I copied software from friends/relatives.

4. Do you use a home computer to complete work-related assignments?

Yes _____ No _____

5. How do you transfer data between home and office?

Diskette _____ Modem _____ Portable Computer _____

6. Who provided the software used at home for work-related assignments (check any of the following answers that apply)?

_____ I purchased my own software.
_____ I was reimbursed by my employer for my software.
_____ My employer purchased software for my use at home.
_____ I use a copy of my employer's software for work-related tasks on my home computer.
_____ I downloaded software from the Internet.
_____ I copied it from friends/relatives.

7. What software applications would you like to have at work that you currently do not?

| | |
|---|---|
| Employee | Title |
| Date | Unit/Department |

# GLOSSARY OF COPYRIGHT TERMS[4]

The following terms and definitions provide a basic understanding of copyright law and legal software use.

1. **Client End.** The term "client end" refers to the computer system making requests to be serviced by the server end computer system within a network environment. It may also include the individuals or organizations operating the computer system.

2. **Computer Program.** Under the Copyright Act, a computer program is defined as "a set of statements or instructions to be used directly or indirectly in a computer in order to bring about a certain result." 17 U.S.C. 101.

3. **Concurrent License.** A concurrent license permits a specified number of users to access software installed on a server at any given time. Usually, metering and lockout software is required by the license to be installed on the server to prevent excessive use. For example, a concurrent license may permit any 75 users to access software on a server, at a single point in time, in a 100-user environment. The remaining 25 users are locked out until one of the original 75 log off.

4. **Content.** The term "content" is used to refer to the various types of data that can be displayed by a computer, such as text, sound, images, photographs, and motion pictures. Content should be contrasted with software, which is a set of computer programs used to make the content available to the user.

5. **Copyright.** Copyright is the exclusive right granted to "authors" under the U.S. Copyright Act to copy, adapt, distribute, rent, publicly perform, and publicly display their works of authorship, such as literary works, databases, musical works, sound recordings, photographs and other still images, and motion pictures and other audiovisual works.

6. **Copy.** A copy, as that term is used in the Copyright Act, is any material object, other than phonorecords, in which a work is fixed by any method now known or later developed, and from which the work can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. 17 U.S.C. 101.

7. **Crackz.** The term "crackz" usually refers to material or software designed to circumvent copyright protections in software to facilitate illegal use.



---

4 Source: Software & Information Industry Association (**www.siia.net)**.

**8. Digital Content.** The term "digital content" is used to refer to any information that is published or distributed in a digital form, including text, data, sound recordings, photographs and images, motion pictures, and software.

**9. Display.** To display a copyrighted work means to show an original work or a copy of it, whether directly or by means of a film, slide, television image, or any other device or process or, in case of a motion picture or audiovisual work, to show individual images nonsequentially. 17 U.S.C. 101.

**10. Distribution.** The term "distribution," in terms of copyright law, refers to the exclusive right of the copyright holder to sell, trade, rent, lease, lend, or otherwise transfer material from one entity to another.

**11. Fair Use.** Fair use is a limited doctrine providing for certain exceptions when permission is not required to use portions of copyrighted works. Because most copying of software includes the entire program, its application is rare in this case.

**12. Freeware.** The reproduction and distribution of freeware is allowed and encouraged as long as it is not for profit and with the condition that derivative works must also be designated as freeware. That means that you cannot take freeware, modify or extend it, and then sell it as commercial or shareware software.

**13. Implied License.** The term "implied license" refers to the permission to use a copyrighted work that is implied as a result of some act or conduct on the part of the copyright holder. An implied license is a binding contract between the parties which is agreed to as a result of their conduct, rather than an overt expression of agreement. The determination of an implied license is subjective depending on the circumstances of use of the copyrighted material.

**14. Infringement.** The concept of infringement arises in patent, copyright, or trademark law. When someone copies software without permission of the copyright or patent owner, or uses a trademark without the permission of the trademark owner, he or she has committed an act of infringement, that is, he or she has infringed on the rights of the copyright, patent, and/or trademark owner.

**15. Intellectual Property.** The term "intellectual property" refers to personal rights of ownership acquired originally or derivatively from intellectual creations. For example: copyrights, trademarks, and patents.

**16. License.** A license (or license agreement) is a contract in which a party with proper authority (the "licensor") grants permission for another party (the "licensee") to do something that would otherwise be prohibited.

**17. Licensee.** The licensee is the party who acquires permission to exercise certain rights in software or content, subject to the terms and conditions imposed by the licensor, in a license agreement. A licensee obtains no ownership rights in the copy of the content that he or she receives.

**18. Licensor.** The licensor is the party who grants to another certain limited rights to possess and use software or content.

**19. Patent.** A patent is a grant of exclusive rights issued by the U.S. Patent and Trademark Office that gives an inventor a 20-year monopoly on the right to "practice" or make, use, and sell his or her invention.

**20. Phonorecord.** Phonorecords are material objects in which sounds, other than those accompanying a motion picture or other audiovisual work, are fixed by any method now known or later developed, and from which the sounds can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device. 17 U.S.C. 101. Thus, a compact disc is a phonorecord.

**21. Piracy.** Software piracy is the unauthorized use of software.

**22. Public Display Right.** The term "public display right" refers to the exclusive right granted to the owner of a copyright to display (and to authorize others to display) his or her work publicly. 17 U.S.C. 106(5).

**23. Public Domain.** Public domain software comes into being when the original copyright holder explicitly relinquishes all rights to the software. Since under current copyright law, all copyrighted works (including software) are protected as soon as they are committed to a medium, for something to be public domain it must be clearly marked as such.

**24. Published, Publication.** Publication, under the Copyright Act, is the distribution of copies of a copyrighted work to the public by sale or other transfer of ownership, or by rental, lease, or lending. The offering to distribute copies to a group of persons for purposes of further distribution, public performance, or public display also constitutes publication. A public performance or display of a work does not of itself constitute publication. 17 U.S.C. 101.

**25. Reproduction Right.** The term "reproduction right" refers to the exclusive right granted to the owner of a copyright to make (and authorize others to make) copies of his or her work. 17 U.S.C. 106(1).

**26. Server End.** The term "server end" refers to the computer system servicing the client computer's requests within a network environment. It may also include the individuals or organizations operating the computer system.

**27.** **Server License.** A server license permits all the users and/or workstations connected to a server to access software installed on the server. Other times, a server license specifically permits a set number of users or workstations to access software installed on the server—often called a per-seat or per-node license.

**28.** **Shareware.** The copyright holders for shareware allow purchasers to make and distribute copies of the software, but demand that if, after testing the software, you adopt it for use, you must pay for it.

**29.** **Software.** See also, computer program.

**30.** **Statutory Damages.** Some laws provide a threshold level of damages, called statutory damages. One such statute is the Copyright Act, which provides that the plaintiff may recover between $500 and $100,000 for each copyrighted work infringed by the defendant, regardless of whether he or she is able to prove in court that he or she has actually been damaged. 17 U.S.C. 504.

**31.** **Trademark.** A trademark is any word, name, symbol, or device, or any combination thereof, adopted and used by a manufacturer or merchant to identify his or her goods and distinguish them from those manufactured or sold by others. 15 U.S.C. 1127.

**32.** **URL.** The term "URL" is an acronym for uniform resource locator. It is the address of a site on the Internet and tells the client software where to locate a sought after file.

**33.** **User.** See also, client.

**34.** **Warez.** The term "warez" refers to pirated or illegal software. Software or sites labeled as warez usually contain illegal material and should be avoided and reported.

**THE WHITE HOUSE**

**Office of the Press Secretary**

For Immediate Release October 1, 1998

Executive Order 13103

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 record keeping 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.

Section 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.



Section 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.

Section 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.

Section 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)).

Section 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.

Section 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.

Section 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.

Section 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.

WILLIAM J. CLINTON

THE WHITE HOUSE,
September 30, 1998