

## **SAMPLE ORGANIZATION SOFTWARE POLICY**

### **Part 1. General Responsibilities**

The Policy of [organization] is to manage its software assets to derive maximum benefit to [organization] and its employees and, especially, to ensure that [organization] and its employees:

- Acquire, reproduce, distribute, transmit, and use computer software in compliance with international treaty obligations and [insert country name] laws, including the [insert specific key laws]; and
- Maintain only legal software on [organization's] computers and computer networks.

All software is protected under [country specific] copyright laws from the time of its creation. [Organization] has licensed copies of computer software from a variety of publishers to help fulfill its mission. Unless otherwise provided in the software license, duplication of copyrighted software, except for backup and archival purposes, is a violation of the [applicable law] and this Policy.

You may not knowingly use software for which [organization] lacks the appropriate license. If you become aware of the use or distribution of unauthorized software in this organization, notify your supervisor or the Office of the Chief information Officer (CIO).

You may not loan or give to anyone any software licensed to this organization.

The licenses for some of this organization's software permit employees of the organization to make a copy of the software for home use. The CIO may approve such use by employees that can demonstrate a need to conduct the organization's business from their homes. Under no circumstances, however, may an employee use the organization's software for purposes other than the business of this organization.

No employee may use or distribute personally-owned software on the organization's computers or networks. Such software threatens the integrity and security of the organization's computers and networks.

A variety of software is available on the Internet. Some of this software, called "freeware" or "shareware," is available free of charge for limited use and may be downloaded to your computer with the prior written approval of your supervisor. 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. No employee shall download such software to his or her computer without the prior written approval of the CIO.

### **Part 2. The Software Asset Management Process**

[Organization] is committed to managing its software assets for maximum benefit to the organization and its employees. The process consists of three areas of focus: (1) Creating an environment in which the process will succeed, (2) Reviewing the software assets residing on the organization's computers, and (3) Acting to correct breaches in policy and the law, keep the Policy and its procedures current, and prevent future breaches.

[Organization] will strive to create an environment for success by communicating this policy; educating employees about their responsibilities; training employees in the software supported by this organization; identifying and modifying as necessary the software employees need to fulfill

their job responsibilities; establishing a secure repository for original storage media, software licenses, and software documentation; and requiring that all software be procured through official and clearly defined procedures.

As part of this organization's software management process, the CIO shall conduct periodic, random reviews of all organization computers and networks to determine the software resident on such systems and whether the organization has the appropriate licenses for all such software. The CIO also shall conduct periodic, planned reviews, in which the CIO may ask you to complete a Software User Survey. This Survey will be used to determine your existing and future use and need of particular software programs. Your cooperation with all reviews and Software User Surveys is greatly appreciated. The CIO will endeavor to conduct its work with the least possible disruption of your workday.

You may be held responsible for the existence of any software on your computer for which the organization lacks the appropriate licenses. Consequences for such unauthorized use of software range from a reprimand for minor offenses to termination of employment for repeated, willful offenses.

### **Part 3. Software Procurement and Installation Procedures**

All requests for software and software upgrades shall be submitted to the Office of the Chief Information Officer (CIO), where possible.

Any software and software upgrades not acquired by the CIO shall be documented and identified to the CIO, who will verify that the Agency has an appropriate license for the use of such software.

All acquisitions of hardware that include bundled software shall be documented and identified to the CIO, who will verify that the Agency has an appropriate license for the use of such bundled software.

The CIO shall store in a secure, central location all original software licenses, disks, CD-Roms, and documentation upon receipt of all new software, including copies of completed registration cards.

The CIO shall designate those employees authorized to install software on the organization's computers.

No employee shall install or distribute software for which this organization lacks the appropriate license.

No employee shall install any software upgrade on a computer that does not already have resident on it the original version of the software. The CIO or designated employee shall destroy the original version's backup copy of the upgraded software in its place.

The CIO or designated employees shall destroy all copies of software that is obsolete or for which the organization lacks the appropriate license. Alternatively, the CIO may obtain the license(s) necessary to maintain unauthorized software on organization computers.

The organization's department with procurement responsibility must establish and maintain a recordkeeping system for software licenses, hardware, original CD-ROMs and diskettes, user

information, and review information. Maintain this information in a secure, central location. Consider the use of software management computer programs to automate such recordkeeping.

\* \* \* \* \*

The organization is committed to communicating this Policy with its employees. The organization will:

- Distribute include the Policy Statement in the employee handbook, and distribute the updated handbook to all employees.
- Train new employees during their initial orientation on how to comply with the Policy.
- Hold seminars on the Software Policy for existing employees to inform them of the types of software licenses, how to detect and prevent piracy, how to implement the Software Policy, and consequences of violating the Policy and relevant law.
- Require new and existing employees whose responsibilities include the installation, maintenance, or oversight of information technology systems to acknowledge and sign the Software Policy Statement.
- Circulate reminders of the Policy on a regular basis (at least annually) or remind employees of the Policy in other ways (at least annually), for example, through notices in agency newsletters.
- Inform employees where they can get additional information on the Policy and software theft prevention.

If you have any questions concerning this Policy or your obligations under it, you may direct them to either your supervisor or the CIO (provide phone numbers, office locations, and e-mail addresses).

**Employee acknowledgement of understanding and responsibility:**

Printed Employee Name: \_\_\_\_\_

Employee Signature and Date: \_\_\_\_\_

