

BUSINESS SOFTWARE ALLIANCE

**SOFTWARE MANAGEMENT GUIDE**



# INTRODUCTION

**IN TODAY'S DIGITAL ECONOMY, COMMERCIAL** software is indispensable to every organization, large and small. Thanks to software, your business is more efficient and your workers more productive, and you can take advantage of all the benefits e-commerce offers.

But to get the most out of your software, you have to manage it well, just as you would any other valuable company asset. Poor software management robs your company of the full value of the productivity and efficiency of software. Poor software management can also easily mask software piracy, which is the installation or use of unauthorized copies of software. Software piracy is against the law and can have very costly consequences to your business.

Illegal software is more likely to fail, rendering your computers and their information useless. You can expect no warranties or support for unlicensed software, leaving your company on its own to deal with failures.

There are legal consequences as well, including stiff civil penalties and the risk of criminal prosecution. The software industry is vigilant and vigorous in protecting the intellectual property of software developers. Software pirates increase costs to users of legitimate, authorized software and decrease the capital available to invest in research and development of new software.

The Business Software Alliance (BSA) stands ready to help your business avoid these serious problems with sound software management practices. This overview covers the following topics so you can better understand why a software asset management program will benefit your company and how you can implement your own program:

- The Benefits of Effective Software Management
- The Risks of Illegal Software Use
- How to Manage Software Properly
- Preventing Software Piracy in the Workplace
- Glossary
- Sample Corporate Software Policy
- Sample Memorandum to Employees
- Sample Software Needs Analysis Form

# BENEFITS

The Benefits of Effective Software Management

## MANAGING YOUR COMPANY'S SOFTWARE AS A VALUABLE ASSET HAS ADVANTAGES

The most significant is cost control. Software can represent 25 percent of an organization's information technology budget. So it makes good fiscal sense to keep a close eye on what you spend to acquire software, to support and train your staff to use it, and to obtain the hardware you need to make it work. A good plan means your company buys only the software that it needs, ensures employees only use properly licensed software, pays to upgrade only what's being used, and enjoys volume discounts by planning purchases and upgrades.

The key to cost control is budgeting for software as a separate expenditure line item. There are two benefits to this. First, you can plan software purchases and upgrades in an orderly way. With a separate software budget, you can anticipate needs and avoid excessive spending or unexpected costs. Second, having a software budget enables you to track purchases accurately so that you can more easily spot unauthorized copies of software in your enterprise.

By purchasing only the authorized software you need, you cut down on upgrade costs as well. Because you know what products are being used and in what quantity, you upgrade only those copies where the new features will be of use. A coordinated upgrade policy ensures that your entire business keeps pace with industry standards and technology improvements.

Controlling software purchases and upgrades can mean savings on hardware as well. By placing software only on the computers of employees who need it, you can avoid having to upgrade, add, or replace hardware for employees who don't need the capacity. And by deleting unneeded software from your computers, you free up space for data or other software and avoid having to add storage space.

By planning software acquisitions and upgrades, you can help your employees anticipate change during the year through notification of new software installations. The planning process also accounts for any training and support that will be needed (as new software or employees are introduced), resulting in employees that are better prepared, and more efficient and productive.

So, proper software management saves time and money, makes employees more productive, keeps software and information compatible throughout the business, and makes it easier for your business to adapt to change.

# RISKS

The Risks of Illegal Software Use

## USING UNLICENSED SOFTWARE CAN RESULT IN SERIOUS CONSEQUENCES

Just like movie videotapes or audio CDs, computer software is intellectual property that's owned by the people who created it. Without the express permission of the manufacturer or publisher, it is illegal to use software, no matter how you got it. That permission almost always takes the form of a license from the publisher, which accompanies authorized copies of software. When you "buy" software, what you're really doing in almost every case is purchasing a license to use it. Rather than owning the software, you acquire limited rights to use, reproduce, and distribute the program, according to the terms spelled out in the license.

Typically, a licensed copy of a program can be installed and used on only one computer at a time, although there are usually provisions allowing you to make a backup copy for archival or disaster recovery purposes. If you don't comply with the terms of the license — for example, by installing the same copy of a single-user program on several computers — that's software piracy. The publisher can take legal action against you or your business.

The license isn't the only way in which software is protected. Copyright, and sometimes patent law, protects software from unauthorized copying, distribution, and sale. The law describing these copyrights and their limitations is included in Title 17 of the U.S. Code. Potential penalties for infringers are listed in both Title 17 and Title 18. The law also recognizes the Internet and prohibits users from uploading, downloading, or transmitting unauthorized copies of software online. An individual who breaks these laws, or a company that looks the other way when an employee does, has civil and criminal liability. The consequences range from significant civil damages to criminal fines and even the possibility of imprisonment.

Using illegal copies of software has other serious consequences. Software publishers offer their legitimate customers a wide array of services besides the copy of the program itself: user manuals and other documentation, notification of problems, training, support services, repairs, and upgrades. A legitimate copy ensures that you're getting a quality product produced by the rightful owner of the program.

An illegal copy provides none of these benefits. Further, it could well be an outdated version of the software, a test copy with bugs, an improperly made copy that can damage or compromise data or a copy hiding a damaging virus capable of jeopardizing the security of an organization's computer network. Any one of these problems could quickly escalate into costly damages that become far more expensive than the money you "saved" by buying or downloading illegal software. Protection from these risks also requires the use of proven cyber security software and, in the case of organizations, the adoption of strong security policies and the use of trained security professionals.

Unlicensed software cheats its creators out of their fair reward for the innovation they have created and cheats your company out of the full value of the software. And it could well damage your data, subject you to fines or even land you in prison. In short, using pirated software is bad business for everyone.

It is important to educate employees on the role they play in protecting their company against security breaches. Senior management needs to play an active role in the information security programs of their organizations in order for them to be effective. The following security tips are important to keep in mind:

- **Install Anti-Virus Software:** Ensure that all computers have anti-virus software installed. Make sure the automatic update feature is activated.
- **Be Cyber Secure:** Report cyber attacks to local law enforcement agencies and your IT provider.
- **Install a Firewall:** A firewall will protect your computer(s) from unauthorized access and use by hackers.
- **Check for Security Updates:** Security updates should be checked every 30 days for programs installed on computers and operating systems. Allow for automatic updating and/or subscribe to a notification service provided by the vendor.
- **Computer Passwords:** Change computer passwords every 120 days and make sure they are strong passwords that contain numbers and symbols.
- **Employee Communication:** Talk to employees about the importance of being cyber secure.

## MANAGING SOFTWARE WELL IS A FOUR-STEP PROCESS

### Step One: Develop Policies and Procedures

Before anything else, your company culture must be one in which all your employees understand the value of commercial software, learn the difference between legal and illegal use, and commit to proper software use. To do this, your organization must have a clear statement of policy. The statement should express the company's goals to manage software for maximum benefit, deal only in legal software, and spell out the company's procedure for acquiring legal software. An effective software purchase procedure consists of the following elements:

- Centralize all your purchases through a purchasing department or other designated company authority;
- Require that all software purchase requests be in writing with department manager approval;
- Ensure the software being requested is on the company's list of supported software;
- Buy only from reputable, authorized sellers;
- Work only with reputable Application Service Providers (ASPs), and ensure you maintain all relevant licenses and documentation with that ASP;
- Get original user materials (e.g., manuals, registration cards, etc.), licenses, and receipts for each purchase;
- Don't permit employees to buy software directly or charge it to their expense accounts;
- Ensure that legal software cannot be downloaded from the Internet by employees without special approval; and
- Don't permit employees to download peer-to-peer (P2P) client software that may be used for trading copyrighted works.

There is a sample corporate policy statement at the back of this booklet for your company to consider adopting as its own. Whatever your policy, make sure it is included in the packet of information given to new employees, distributed to all current employees, posted on company bulletin boards, and available on company computer networks. Every employee needs to acknowledge the statement of policy and the consequences of violating it. In turn, employers must take steps to educate employees on what constitutes illegal use of software.

In developing internal procedures for software asset management, every company should ask itself the question: "What software do we need?" The answer will always be valuable in ensuring effective and efficient purchasing and use of software and in guiding your efforts to establish and maintain compliance.

As a general principle, your procedural analysis should answer the following questions:

- Are you using the right software in terms of efficiency and effectiveness?
- Are staff satisfied with their current software applications?
- Are there other software programs that would enable staff to operate in a more effective and efficient manner?
- Are there software programs you currently possess but don't need any longer?

Your organization's procedures should include identifying the appropriate software profile for each computer by assessing whether department/staff members need alternative or additional software applications. Also, software that is not being used should be identified to determine whether your company wants to maintain that program.

### **Step Two: Audit Your Software**

Once you have a policy and a set of procedures in place, your next step is to take inventory of your software assets. Only by knowing what programs are installed on all the computers in your organization — desktops, laptops, and any copies of programs from work installed by employees on their home computers — can you determine how to proceed.

An accurate inventory can answer the following questions:

- Are we using the most recent or most suitable version of programs we need?
- Are we using outdated or unnecessary programs that can be deleted?
- Are there other programs we should obtain to become more productive or efficient?
- Does each employee have the correct set of available programs?
- Are employees properly trained to use the software we have?
- Do we have illegal, unauthorized, or unlicensed programs or copies in our business?

There are many tools available to help you complete the inventory or you can do it manually. BSA's Web site, [www.bsa.org](http://www.bsa.org), provides software audit tools free of charge to your business. No matter what tools you use, make sure to collect the following information for each copy of software installed on each computer:

- Product Name
- Version Number
- Serial Number

You should also take an inventory of material related to software on your computers, including:

- All floppy disks, CDs, or other storage media used to install the programs on your computers;
- All original manuals and reference documentation;
- All license documentation; and
- All invoices, proofs of purchase, and other documents proving the legitimacy of your software. This includes invoices for computer systems that were sold to you with software already installed.

Once the inventory is complete, you should carefully store the documentation, original copies of your software, and other material in a secure place. That way, you can take advantage of services, upgrade offers, and the like from publishers, and reinstall software more easily.

### **Step Three: Determine What's Legal or Illegal**

With your inventory in hand, you can compare the software that's installed on your company's computers to what's allowed under the terms of your licenses. Remember that some licenses allow you to make a certain number of copies of a program from a single source or to have a limited number of network users use the software simultaneously. The original license will tell you how many.

Once you have identified any illegal software copies in your organization, you should delete them from your computers. This is also an ideal time to remind employees about the company's software policy and the dangers associated with unlicensed software.

Now you can compare the legitimate copies of software that remain on your computers with the corporate needs that you identified when taking the inventory. You can make informed decisions about which software you legally have that you want to keep, upgrade, or discard. Programs can be moved — not copied — from computers where they are not needed to computers where they are. Programs can be upgraded, if necessary, so that everyone is using the version of the program that's most appropriate for your company. And you can purchase only the new, legitimate software you need.

Based on the inventory, upgrades, new purchases, and input from employees, you can now create a formal list of the software that your company will allow its employees to use. It should include program names, serial numbers, version numbers, number of copies or users permitted by the license, the computers on which the copies are installed, and plans to add, upgrade, or discard the software in the future.

#### Step Four: Establish a Routine Audit

Effective software management is a continual process. You need to monitor adherence, guard against the introduction of illegal software, keep your list of supported software up to date, and plan ahead for the next three years. It makes sense to have someone within your company responsible for the process in order to centralize the job.

Periodically, it's a good idea to perform spot checks on individual computers to make sure illegal software has not been inadvertently or deliberately installed. It also makes sense to conduct an inventory at least every year, just as you might for other valuable assets. When employees leave the company, make sure the software they worked with remains with your company and that they do not take or keep copies.

## UNDERSTANDING PIRACY PREVENTION IS SIMPLY A BUSINESS "BEST PRACTICE"

After you've put your software assets in good order, you'll still need to monitor your workplace for illegal software. There are five common types of software piracy, and understanding each will help you and your employees avoid the problems of illegal software.

#### End-User Piracy

End-user piracy occurs when an employee reproduces copies of software without authorization. End-user piracy can take the following forms:

- Using one licensed copy to install a program on multiple computers;
- Copying disks for installation and distribution;
- Taking advantage of upgrade offers without having a legal copy of the version to be upgraded;
- Acquiring academic or other restricted or nonretail software without a license for commercial use; and
- Swapping disks in or outside the workplace.

These practices must be prohibited.

The lion's share of the losses due to software piracy comes from the relatively pedestrian problem of over-installation — that is, loading a program onto more workstations than is authorized by the license agreement. Piracy not only deprives software creators of a return on their investment, it costs jobs in related businesses, hurts the economy, and deprives the consumer of new products.

Technological measures to stem the growth of piracy are rapidly becoming a mainstream option for many software companies. Technologies such as product activation help to ensure compliance with end-user license agreements, while minimizing the impact on legitimate users. One simple step in the installation process is often all it takes both to enable full use of a software program and to prevent its unauthorized installation. Product activation technologies that are fast, nonintrusive, anonymous, and flexible can help combat piracy without unduly burdening users.

### Client-Server Overuse

Client-server overuse occurs when too many employees on a network are using a central copy of a program simultaneously. If you have a local-area network (LAN) and install programs on the server for several people to use, you have to be sure your license entitles you to do so. If you have more users than allowed by the license, that's overuse. You can correct this problem by making sure employees understand the restrictions, by installing "metering" software that ensures only the licensed number of users have access, or by purchasing another license that covers the number of users you need.

### Internet Piracy

The software industry plays a leading role in ensuring that the Internet reaches its full potential. Commercial software publishers have contributed in countless ways to the Internet's success, providing the means by which content can be created, displayed, and exchanged and providing some of the most desired content itself. However, intellectual property theft on the Internet constrains the software industry and significantly reduces its positive impact on economies throughout the world. There are thousands of pirate Web sites located on the Internet, and virtually every commercial software product now available on the market can be located on one of these sites. Hence, Internet piracy represents perhaps the single greatest threat to electronic commerce.

The same laws and license agreements that apply to software in physical distribution channels also apply to cyberspace and Internet transactions. The U.S. Copyright Act does not differentiate between offline and online infringement. Both are prohibited and subject to criminal prosecution and civil penalties, including statutory damage awards of up to \$150,000 per copyrighted work.

While there are many publishers who offer authorized versions of their software for sale online, there are also numerous pirate operations on the Internet as well:

- Pirate Web sites that make software available for free download or in exchange for uploaded programs;
- Internet auction sites that offer counterfeit, out-of-channel, or infringing copyright software; and
- Peer-to-Peer (P2P) networks that enable unauthorized transfer of copyrighted programs.

The purchasing rules that apply to software purchased through traditional means should also apply to online software purchases. Organizations should have a clear policy as to when, whether, or with whose authorization employees may download or acquire software from Internet sites.

**B**elow are tips to help the public and businesses when purchasing software online from auction sites, discount retailers, or in response to e-mail solicitations:

- If a price for a software product seems "too good to be true," it probably is;
- Be wary of software products that come without any documentation or manuals;
- Beware of products that do not look genuine, such as those with handwritten labels;
- Beware of sellers offering to make "backup" copies;
- Watch out for products labeled as academic, OEM, NFR, or CD-R;
- Be wary of compilations of software titles from different publishers on a single disk;
- Do not give out your credit card details unless you know it's a secure transaction; and
- Check with organizations such as BSA should you become a victim of software fraud.

### Hard-Disk Loading

Hard-disk loading occurs when the business that sells you a new computer loads illegal copies of software onto its hard disk to make the purchase of the machine more attractive. The same concerns and issues apply when you engage a Value Added Reseller (VAR) to sell or install new software onto computers in your office. You can avoid purchasing such software by ensuring that all hardware and software purchases are centrally coordinated through your organization and all purchases are made through reputable suppliers. Most importantly, require receipt of all original software licenses, disks, and documentation with every hardware purchase.

## Software Counterfeiting

Software counterfeiting is the illegal duplication and sale of copyrighted material with the intent of directly imitating the copyrighted product. In the case of packaged software, it is common to find counterfeit copies of the CDs or diskettes incorporating the software program, as well as related packaging, manuals, license agreements, labels, registration cards, and security features. Sometimes it is clear the product is not legitimate, but often it is not. Look for the following warning signs:

- You're offered software at a price that appears "too good to be true";
- The software comes in a CD jewel case without the packaging and materials that typically accompany a legitimate product;
- The software lacks the manufacturer's standard security features;
- The software lacks an original license or other materials that typically accompany legitimate products (e.g., original registration card or manual);
- The packaging or materials that accompany the software have been copied or are of inferior print quality;
- The software is offered on an auction site;
- The CD has a gold appearance, rather than the silver, blue, or green appearance that characterizes a legitimate product;
- The CD contains software from more than one manufacturer or programs that are not typically sold as a suite; and/or
- The software is distributed via mail order or online by sellers who fail to provide appropriate guarantees of a legitimate product.

Proper software management takes some time and effort, but the payback is well worth it. If you have followed the process outlined in this guide, you have taken the steps necessary to get the full benefit from your software — and to eliminate your company's exposure to penalties for illegal software use.

The Business Software Alliance (BSA) provides resources, tools, and tips about the importance of software compliance and using fully licensed software.

BSA is the foremost organization dedicated to promoting a safe and legal digital world. BSA is the voice of the world's commercial software industry before governments and in the international marketplace. Its members represent one of the fastest-growing industries in the world. BSA educates consumers on software management and copyright protection, cyber security, trade, e-commerce, and other Internet-related issues.

BSA's Web site, [www.bsa.org](http://www.bsa.org), offers a variety of information on software management, security, policy initiatives, and copyright issues around the globe. BSA also operates 65 anti-piracy hotlines around the world for those reporting suspected software theft.

# GLOSSARY

## Application Software

General term for software programs that perform specific tasks such as accounting, word processing, and database management.

## CD-R

A type of optical disk capable of storing large amounts of data — up to 1GB (gigabyte), although the most common size is 650 MB (megabytes). This differs from a CD-ROM, in that you can write data to it. Commercial software is not distributed on CD-Rs.

## CD-ROM

A type of optical disk capable of storing large amounts of data — up to 1GB (gigabyte), although the most common size is 650MB (megabytes). Most commercial software is distributed on CD-ROM. Most CD-ROMs are read-only storage media best suited for holding reference information, which does not change on a daily basis and is not subject to being updated by those who use it.

## Channel

The route via which the software makes it to the end-user. It usually involves the distribution from the publisher to large distributors and then to the resellers. The resellers then supply the software to the end-user.

## Copyright

The legal rights of an author under federal law (Title 17 of the U.S. Code) to control the reproduction, distribution, adaptation, and performance of his/her work, including software. The copying of a copyrighted work without the permission of its author may subject the copier to both civil and criminal penalties.

## Diskette

A flat piece of flexible plastic covered with a magnetic coating, which is used to store data (also called a floppy disk). The existing standard for diskette size is 3 1/2 inches. Unlike hard disks, floppy disks are portable and can be removed from a disk drive.

## Download

To move a file from a computer at another site to your computer over a communications line. The term is often used to describe the process of copying a file from the Internet to a computer. Downloading can also refer to copying a file from a network file server to a computer on the network.

## End-User

The final or ultimate user of a computer system and/or product.

## File Transfer Protocol (FTP)

FTP is the standard computer language that allows disparate computers to exchange files quickly and easily, including the uploading and downloading of software programs. Computers established as FTP sites can contain enormous quantities of program files, along with other information. When exploited by software pirates, they facilitate the distribution of large volumes of copyrighted software programs.

## Fixes

Corrections to vendor-supplied software. The vendor does not necessarily supply these fixes.

## Hard Disk

A magnetic disk on which you can store computer data (also called a hard drive). Unlike floppy disks, hard disks cannot be easily removed from the computer and, hence, are not portable. Hard disks hold more data and are faster than floppy disks. A hard disk, for example, can store anywhere from 10 megabytes to several gigabytes, whereas most floppy disks have a maximum storage capacity of 1.4 megabytes.

## Hardware

The physical components of a computer system.

## Intellectual Property Rights

The legal rights persons have to prevent others from using without permission certain kinds of intangible property. The objective of laws protecting intellectual property rights is to promote innovation and creativity. These laws take a number of different forms, including laws protecting “patents,” which govern rights in inventions; “copyrights,” which govern rights in software, books, movies, and music; “trademarks,” which protect the reputation of the entity that owns a mark; and “trade secrets,” which safeguard valuable business information.

## LAN

Local-area Network. A computer network that spans a relatively small area. A LAN lets you share files as well as devices such as printers or CD-ROM drives. A LAN can be connected to other LANs over any distance via telephone lines and radio waves; a system of LANs connected in this way is called a wide-area network (WAN).

## License

A legally binding agreement in which one party grants certain rights and privileges to another. In the computer field, a software publisher will typically grant a nonexclusive right (license) to a user to use one copy of its software and prohibit further copying and distribution of that software to another user.

## Modem

A device or program that enables a computer to transmit data over telephone or cable lines.

**NFR**

NFR (not for resale) is software that is distributed by some publishers for demonstrations or other limited purposes.

**Network Operating System**

An operating system that includes special functions for connecting computers and devices into a local-area network (LAN). A network operating system coordinates a network's primary functions such as file transfer and print queuing.

**OEM**

OEM (original equipment manufacturer) is distributed with hardware, generally a new PC. The license usually prohibits distribution without a new PC.

**Operating System**

The master control program that translates the user's commands and allows application programs to interact with the computer's hardware. Every general-purpose computer must have an operating system to run other programs. Operating systems perform basic tasks, such as recognizing input from the keyboard, sending output to the display screen, keeping track of files and directories on the disk, and controlling peripheral devices such as disk drives and printers. Common operating systems include DOS, Windows, and Mac OS.

**Peer-to-Peer (P2P)**

P2P technology allows users to locate, share, and distribute information between workstations without connecting to a central server. Although P2P has a lot of legitimate uses, it has become one of the more popular ways to share copyrighted materials, including software, over the Internet.

**Piracy**

The illegal use and/or distribution of property protected under intellectual property laws. Software piracy can take many forms. End-user piracy occurs when an individual or organization reproduces and/or uses unlicensed copies of software for its operations. Client-server overuse occurs when the number of users connected to or accessing one server exceeds the total number defined in the license agreement. Counterfeiting is the illegal duplication of downloaded software with the intent of directly imitating the copyrighted product. Hard-disk loading occurs when a computer hardware reseller loads unauthorized copies of software onto the machines it sells. Online software theft occurs when individuals download unauthorized copies of software from the Internet. License misuse occurs when software is distributed in channels outside those allowed by the license, or used in ways restricted by the license.

**Product Activation**

A process used by software publishers to help end-users verify that software is legitimately licensed, to ensure that the software they are using is genuine, and to deter unauthorized copying.

**Server**

A computer or device on a network that manages network resources. For example, a file server is a computer and storage device dedicated to storing files. Any user on the network can store files on the server. A print server is a computer that manages one or more printers, and a network server is a computer that manages network traffic. A database server is a computer system that processes database queries.

**Software**

Computer instructions or data. A piece of software is also known as a program.

**System Software Products**

Software program packages, other than application program packages, that manage systems resources (e.g., operating systems, database management systems, etc.).

**Upgrade**

A new version of a software or hardware product designed to replace an older version of the same product. Typically, software companies sell upgrades at a discount. In most cases, you must prove you own an older version of the product to qualify for the upgrade price.

**Upload**

To move a file from your computer to another computer; the opposite of download.

**WAN**

Wide-area Network. A computer network that spans a relatively large geographical area. Typically, a WAN consists of two or more local-area networks (LANs). Computers connected to a wide-area network are often connected through public networks, such as the telephone system. They can also be connected through leased lines or satellites.



Business Software Alliance  
1150 18th Street, NW, Suite 700  
Washington, DC 20036  
Tel: 202.872.5500  
Fax: 202.872.5501  
Hotline 1.888.NO.PIRACY

BSA Europe/Middle East/Africa  
79 Knightsbridge  
London, SW1X 7RB  
England, United Kingdom  
Tel: +44 (0) 20.7245.0304  
Fax: +44 (0) 20.7245.0310

BSA Asia  
300 Beach Road  
#32-07 The Concourse  
Singapore 199555  
Tel: + 65.6.292.2072  
Fax: + 65.6.292.6369