

Guide to software piracy prevention

Siemens PLM Software/ Siemens Industry Software

Introduction

This guide has been designed to help your business ensure the legal use of Siemens software. It discusses the issue of software piracy, the risks of using unlicensed software, outlines Siemens' software licensing policy and provides information to help your business avoid potential problems by implementing sound software asset management practices.

What is the law regarding software piracy?

Software development involves the creative ideas and talents of programmers, writers and graphic artists. Similar to most creative works, such as books, movies and films, computer software is copyrighted material protected by the laws of each country in which it is licensed and international treaties. Copyright laws provide the copyright owner the exclusive right to make copies of, distribute, license and sell its software and the exclusive right to develop new software incorporating the original copyrighted work.

The software owner grants to others the right to use the software, typically under the terms of a license agreement. If you copy, distribute or install the software in ways that the license does not specifically authorize, whether you are sharing disks with coworkers and friends or participating in widespread duplication, you are violating copyright law. If you assist another person make unauthorized copies, you are also liable under copyright law.

Making or downloading unauthorized copies of software is breaking the law, no matter how many copies are involved. You are committing copyright infringement if you are duplicating software to sell, making multiple copies for use by different users within your organization or business, giving an unauthorized copy to another individual or lending a copy to a friend. It's still infringement even if you don't make any money doing it.

What are the penalties for pirating software?

Software piracy is stealing. If you or your company are caught using software without a license, you could be held liable under both civil and criminal law. The law enables the copyright owner to stop you and your company from using its software immediately and to obtain monetary damages. The copyright owner may then choose between actual damages, which includes the amount it has lost because of your infringement (as well as any profits attributable to the infringement), and statutory damages, which in the U.S., for example, can be as much as \$150,000 for each program copied. In addition, the government where the infringement is occurring can criminally prosecute you for copyright infringement. If convicted in the U.S., you can be fined up to \$250,000, or sentenced to jail for up to five years, or both.

In addition to termination for breach of contract and the legal consequences noted above, users of pirated or counterfeit software could experience:

- Exposure to unacceptable levels of cyber-security risk,* including malware and viruses
- Inadequate or no documentation
- Void warranties
- Lack of technical product support available to licensed users
- Ineligibility for software upgrades offered to properly licensed users

Companies, both large and small, can be held liable for their employees' actions. If an employee is installing unauthorized software copies on company computers or acquiring illegal software

through the Internet, the company's Managing Director, Chief Executive Officer or Principal can be held liable for copyright infringement – even if the company's management was unaware of the employees' actions. In Russia, for example, the company director's name appears on the criminal complaint and may be released to the press, and most countries around the world impose a similar process.

How does Siemens PLM Software/Siemens Industry Software license its software?

Companies and individuals that acquire Siemens software become licensees – not owners – of the software and obtain only those rights specifically granted in the associated Siemens license agreement. You must have a valid license for each item of software installed. Siemens offers a variety of software licenses, such as "node locked," "floating" and "named user."

- *Node Locked*: Installation and use of software is restricted to a customer specified workstation.
- *Floating*: Installation and use of software is controlled by a customer specified license server with access limited to the number of concurrent users licensed.
- *Named User*: Installation and use of software is restricted to the individual named user identified by the license management system.

Software license fees are based on the type of license and the number of users licensed. Siemens only authorizes customers to copy the software as reasonably required in conjunction with their licensed use of the software and

for backup purposes. The licenses granted are nontransferable and may not otherwise be assigned or used in a country or location other than originally licensed without Siemens' express written consent.

What is the economic impact of software piracy?

Piracy has a number of economic impacts, including affecting the competitiveness of Siemens' customers that have legitimately licensed Siemens' software and compete against those companies or individuals with an unfair advantage that have not.

An independent study on global software piracy reports in-country piracy rates ranging between 20 and 93 percent and highlights the serious impact of such copyright infringement with piracy losses of more than \$58 billion worldwide in 2010.** The study also found that reducing the global piracy rate for PC software by 10 percentage points over four years would create \$142 billion in new economic activity globally while adding nearly 500,000 new high-tech jobs and generating \$32 billion in new tax revenues for governments.

How can businesses manage their software properly?

Like all new initiatives, proper software asset management takes time and effort to establish. However, the long term benefits of the security and protection it affords is easily justified when compared to the risks and penalties of not doing so. To ensure the legal use of software in your organization and your supply chain:

1. Commit, as an organization, to supplying original, genuine software to meet the software needs of all computer users within the organization and ensure that only authentic Siemens-provided license files are installed.
2. Identify the appropriate software profile for each computer user. Create a formal list of 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 copies are installed, and plans to add, upgrade or discard the software in the future.
3. The Siemens software license, for example, requires licensees to track installations for its software and, when requested, provide that information to Siemens. So, keep accurate and current records of the machine ID for each installation of Siemens software and log users permitted access.
4. Set realistic budgets for software and hardware.
5. Ensure users have an open, seamless, and clearly communicated process to procure and receive software.
6. Communicate your organization's commitment to the use of licensed legitimate software.
7. Enforce compliance by providing training of users on corporate policies and procedures related to legal software use and conducting periodic audits. Take appropriate steps if unauthorized copies are found.

8. Keep all CDs or other storage media used to install the programs on your computers; all original manuals and 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.
9. Require your supply chain to do likewise.

What can your business do to prevent piracy?

For more information about Siemens' piracy prevention program, please contact us at piracy.aud@siemens.com or log on at www.siemens.com/plm/piracyprevention.

For additional information about the fines and penalties in your jurisdiction associated with software piracy, to learn more about proper software asset management and the BSA's SAM Advantage training course, the first such course aligned to ISO standards for software asset management, to obtain a free software management guide, or to report piracy, call the toll-free BSA Anti-Piracy Hotline at 1-888-NO PIRACY or log on at www.bsa.org. Siemens PLM Software is a worldwide member of the

BSA, a non-profit trade association that represents the nation's leading commercial software manufacturers.



* For more information, see "Software Piracy on the Internet: A Threat To Your Security" at www.bsa.org/country/Research%20and%20Statistics.aspx.

** "Eighth Annual BSA and IDC Global Software Piracy Study" conducted by IDC, May 2011

© 2011 Siemens Product Lifecycle Management Software Inc. All rights reserved. Siemens and the Siemens logo are registered trademarks of Siemens AG. D-Cubed, Femap, Geolus, GO PLM, I-deas, Insight, JT, NX, Parasolid, Solid Edge, Teamcenter, Tecnomatix and Velocity Series are trademarks or registered trademarks of Siemens Product Lifecycle Management Software Inc. or its subsidiaries in the United States and in other countries. All other logos, trademarks, registered trademarks or service marks used herein are the property of their respective holders. BSA is a registered trademark of Business Software Alliance, BSA United States, 1150 18th Street N.W., Suite. 700, Washington, DC 20036. Siemens PLM Software believes the information in this publication is accurate as of the publication date. Such information is subject to change without notice and is subject to applicable technical description. Siemens PLM Software is not responsible for inadvertent errors. Printed in the USA. 8/11 B