|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Software Use and Licensing Policy | | | | | |
| Policy # | CPL-03-03 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888.641.0500 |

**Table of Contents**

[Purpose 1](#_Toc457462839)

[Scope 1](#_Toc457462840)

[Policy 1](#_Toc457462841)

[Copyright Protection 1](#_Toc457462842)

[Software Procurement 1](#_Toc457462843)

[Acceptable Use and Ownership 2](#_Toc457462844)

[Violations 2](#_Toc457462845)

[Definitions 2](#_Toc457462846)

[References 3](#_Toc457462847)

[Related Documents 3](#_Toc457462848)

[Approval and Ownership 3](#_Toc457462849)

[Revision History 3](#_Toc457462850)

Purpose

This policy defines the requirements for compliance with software license agreements and related copyrights on all Company X computer and communications information system. Company X is licensed to use the computer software from a variety of vendors and other sources. Company X does not ***own*** this software or its related documentation and, unless specifically authorized in the license for the software, does not have the right to reproduce it.

Scope

This policy applies to all Company X users and third parties who use proprietary or copyrighted software.

Policy

### ****Copyright Protection****

**Copyright Protection -** All users are required to comply with federal copyright laws, nondisclosure, and vendor licensing agreements governing the installation, use, and distribution of purchased software. All software will be used in accordance with the developer’s license agreements and with the Company X Code of Ethics.

**Copyright License Review –** Company X management must conduct an annual software audit of its computing equipment, comparing the software installed with software proof-of-purchase documentation or the original media (CD-ROM, downloads, etc.)

### Software Procurement

**Software Procurement -** All software used on Company X-owned computers will be purchased through appropriate procedures and from approved vendors. Consult your supervisor or an Information Technology manager for proper procedures.

### Acceptable Use and Ownership

**Remote Worker Usage -** When a user needs to use software for Company business at home, Company X will either confirm that the license allows home use or purchase an additional copy or license.

**Software Ownership -** Anyone issued additional copy(s) of software for home use acknowledges that such additional copy(s) or license(s) purchased for home use are the property of Company X.

**Personal Software Installation -** Users are not permitted to install their personal software (screen savers, utilities, games, etc.) onto Company X computer systems.

**Authorized Use Only -** Users must use software according to the manufacturer license agreements and this policy. Company X licenses the use of computer software from a variety of outside companies, but does not own the copyright to software licensed from other companies.

**Unauthorized Duplication -** Users must not make unauthorized copies of any copyrighted software or intellectual property. Unauthorized duplication of copyrighted computer software violates the law and is contrary to corporate standards of conduct. The Company prohibits this kind of duplication and recognizes the following principles as a basis for preventing its occurrence.

Violations

Any violation of this policy may result in disciplinary action, up to and including termination of employment. Company X reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. Company X does not consider conduct in violation of this policy to be within an employee’s or partner’s course and scope of employment, or the direct consequence of the discharge of the employee’s or partner’s duties. Accordingly, to the extent permitted by law, Company X reserves the right not to defend or pay any damages awarded against employees or partners that result from violation of this policy.

Note: Unauthorized reproduction of software is an International crime, and a Federal offense under both US and Canadian copyright laws. In the United States, for instance, violators may be subject to civil damages in amounts up to $150,000 ***for each instance of each individual title*** copied. (The average Corporate settlement has ranged between 10 million to 12 million dollars) Criminal penalties include fines as high as $250,000 ***for each instance of each individual title*** copied, and imprisonment of up to 5 years.

Definitions

Confidential Information (Sensitive Information) – Any Company X information that is not publicly known and includes tangible and intangible information in all forms, such as information that is observed or orally delivered, or is in electronic form, or is written or in other tangible form. Confidential Information may include, but is not limited to, source code, product designs and plans, beta and benchmarking results, patent applications, production methods, product roadmaps, customer lists and information, prospect lists and information, promotional plans, competitive information, names, salaries, skills, positions, pre-public financial results, product costs, and pricing, and employee information and lists including organizational charts. Confidential Information also includes any confidential information received by Company X from a third party under a non-disclosure agreement

**Information Asset** - Any Company X data in any form, and the equipment used to manage, process, or store Company X data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and partner data.

Third Party (Partner) – Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**User -** Any Company X employee or partner who has been authorized to access any Company X electronic information resource.

References

ISO/IEC 27002: 4.0 Risk Management

CPL: 1.0 - IT Risk Management

NIST: Risk Assessment (RA)

PCI-DSS: 12.2 Annual Risk Assessments

HIPAA: Security Management Process - Risk Management (R)

Related Documents

Approval and Ownership

|  |  |  |  |
| --- | --- | --- | --- |
| Owner | Title | Date | Signature |
| Policy Author | Title | MM/DD/YYYY |  |
| Approved By | Title | Date | Signature |
| Executive Sponsor | Title | MM/DD/YYYY |  |

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Version | Description | Revision Date | Review  Date | Reviewer/Approver Name |
| 1.0 | Initial Version | MM/DD/YYYY | MM/DD/YYYY |  |
|  |  |  |  |  |