|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Acceptable Use of Assets Policy | | | | | |
| Policy # | CPL-04-05 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457917511)

[Scope 1](#_Toc457917512)

[Policy 1](#_Toc457917513)

[System Usage 1](#_Toc457917514)

[User IDs and Passwords 2](#_Toc457917515)

[Electronic Messaging 2](#_Toc457917516)

[Internet and Web Usage 3](#_Toc457917517)

[Data Storage and Copyrights 3](#_Toc457917518)

[Personal Equipment 4](#_Toc457917519)

[Telephones and Voice Mail 4](#_Toc457917520)

[Clear Desks and Clear Screen 4](#_Toc457917521)

[Security Incident Reporting 4](#_Toc457917522)

[Violations 5](#_Toc457917523)

[Definitions 5](#_Toc457917524)

[References 5](#_Toc457917525)

[Related Documents 5](#_Toc457917526)

[Approval and Ownership 6](#_Toc457917527)

[Revision History 6](#_Toc457917528)

Purpose

This policy defines the acceptable use of all Company X computer and communication system assets.

Scope

This policy applies to all employees and third-parties with access to Company X electronic information resources.

Policy

### System Usage

**Reasonable Personal Use Of Systems** - Company X allows computer users to make reasonable personal use of its electronic mail and other computer and communications systems. All such personal use must be consistent with conventional standards of ethical and polite conduct.

**Use at your own Risk -** Workers access the Internet with Company X facilities at their own risk. Company X is not responsible for material viewed, downloaded, or received by users through the Internet. Electronic mail systems may deliver unsolicited messages that contain offensive content.

**Activity Monitoring** – Users must be aware that their internet activity while using Company X systems is monitored and recorded. This information may include web sites visited, files downloaded, time spent on the Internet, and related information.

**No Guarantee of Message Privacy** - Company X cannot guarantee that electronic communications will be private. Workers must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Workers must accordingly be careful about the topics covered in Company X electronic communications.

**Unattended Active Sessions** - Users must not leave their personal computer, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

### ****User IDs and Passwords****

**Personal User IDs Responsibility** - Users must be responsible for all activity performed with their personal user IDs. They must not permit others to perform any activity with their user IDs, and they must not perform any activity with IDs belonging to other users.

**Access Code Sharing Prohibited** - Company X computer accounts, user IDs, network passwords, voice mail box personal identification numbers, credit card numbers, and other access codes must not be used by anyone other than the person to whom they were originally issued.

**Strong Passwords** – Users must choose passwords that are difficult to guess. For example, users must not choose a dictionary word, derivatives of user IDs, common character sequences, details of their personal history, a common name, or a word that reflects work activities.

**Typing Passwords When Others Are Watching** - Users must never type their passwords at a keyboard or a telephone keypad if others are known to be watching their actions. To do so unduly exposes the information accessed thereby to unauthorized access.

**Password Proximity To Access Devices** - Users must never write down or otherwise record a readable password and store it near the access device to which it pertains.

**Passwords In Communications Software** - Users must not store fixed passwords in remote access communications programs, Internet browsers, or related data communications software at any time.

### Electronic Messaging

**Identity Misrepresentation** - Workers must not misrepresent, obscure, suppress, or replace their own or another person's identity on any Company X electronic communications.

**Web Based Mail Systems** - Company X users are prohibited from using any electronic mail system besides that provided by the Information Technology Department. This includes all web-based email systems.

**Handling Attachments** - All electronic mail attachment files from third parties must be scanned with an authorized virus detection software package before opening or execution.

**Responding to Personal Information Requests** – Company X workers must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources. The Company X Information Systems (IS) department will never request that you perform security duties, such as changing your password, via electronic mail. Any such requests will be confirmed with separate communication from management.

**Harassing Of Offensive Materials** - Company X computer and communications systems are not intended to be used for personal use and must not be used for the exercise of the workers’ right to free speech. These systems must not be used as an open forum to discuss Company X organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Workers must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

### ****Internet and Web Usage****

**Disclosing Internal Information -** Workers must not publicly disclose internal Company X by posting to any web site, including blogs, newsgroups, chat groups or social networking sites.

**Offensive Web Sites** - Company X is not responsible for the content that workers may encounter when they use the Internet. When and if users make a connection with web sites containing objectionable content, they must promptly move to another site or terminate their session. Workers using Company X computers who discover they have connected with a web site that contains sexually explicit, racist, sexist, violent, or other potentially offensive material must immediately disconnect from that site.

**Blocking Sites and Content Types** - The ability to connect with a specific web site does not in itself imply that users of Company X systems are permitted to visit that site. Company X may, at its discretion, restrict or block the downloading of certain file types that are likely to cause network service degradation. These file types include graphic and music files.

**Social Networking Sites** – Users are prohibited from accessing web sites designed for the sole purpose of posting and sharing personal information. Exceptions require the approval of the Information Technology Department and must be for documented business purposes. Workers are also prohibited from discussing specific Company X business within any personal home pages they may have established on these sites outside of Company X business hours.

**Instant Messaging** - Company X currently prohibits all use of instant messaging (IM) services, whether internal or external, personal or business. All business communications must be sent through other established means, such as email, fax or telephone.

**Peer-to-Peer** – Use of Peer to Peer (P2P) file sharing software is strictly prohibited on all Company X computer and communication systems.

### Data Storage and Copyrights

**Establishing Third-Party Storage Networks** - Users must not establish any third-party information storage network that will handle Company X information (social media pages, blogs, cloud storage) without the specific approval of the Information Technology Department.

**Unauthorized Software And Data Copies** - Company X strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. Users must not make unauthorized copies of software or other licensed content.

**Copyright Protection** - Company X allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

**Copying to Personal Storage Devices** – Company X users must not copy sensitive Company X business information to personal storage devices, including personal mobile phones, USB drives.

**External Storage Scanning** - Externally-supplied USB drives, CD-ROMs, and other removable storage media must not be used unless they have been checked for viruses.

### ****Personal Equipment****

**Personal Equipment** - Workers must not bring their own computers, computer peripherals, or computer software into Company X facilities without prior authorization from management.

**Use Of Personal Computers** - Workers must not use their own personal computers for production Company X business unless these systems have been evaluated and approved by the Information Technology department.

**Current Virus Software**- Every Company X worker who examines, processes, or stores Company X information using a computer that he or she owns must install and regularly run the most current version of a virus detection software package approved by the Information Technology Manager.

**User Installation Of Software** - Users must not install software on their personal computers, network servers, or other machines without receiving advance authorization to do so from the Information Technology Manager.

**Return of Equipment** – All computer equipment and portable store media (USB, CD-ROM) issued to employees by Company X must be returned to the Information Technology Department when no longer in use.

### Telephones and Voice Mail

**Sensitive Information On Voicemail** - Workers must not record messages containing sensitive client information on answering machines or voice mail systems.

**Voicemail Password Changes** – Employees must change the default password on all voicemail systems.

### Clear Desks and Clear Screen

**Securing Sensitive Information** - When not in use, sensitive information must be protected from unauthorized disclosure. When left in an unattended room, such information must be locked in appropriate containers.

**Clear Desk** – Employees must not leave confidential information lying open on personal desks or workspaces if they are unattended.

**Unauthorized Screen Viewing** - The screens on computers used to handle sensitive information must be positioned such that unauthorized persons cannot readily look over the shoulder of the person using the workstation.

**Unattended Active Sessions** - If the computer system to which they are connected or which they are using contains sensitive information, users must not leave their personal computer unattended without logging out or invoking a password-protected screen saver.

### ****Security Incident Reporting****

**Reporting Security Events** – Any suspected events that may compromise information security or are known to violate an existing security policy must be immediately reported to the Information Technology Manager. Examples of these events include:

* Any unauthorized use of Company X information systems;
* Passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed;
* All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages;
* Suspected or actual disclosure of Sensitive Company X information to unauthorized third parties.

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.

Definitions

**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 –** Any non-employee of Company X who is contractually bound to provide some form of service to Company X.

**Password** **–** An arbitrary string of characters chosen by a user that is used to authenticate the user when he attempts to log on, in order to prevent unauthorized access to his account.

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

References

CPL: 4.5 Acceptable Use of Assets

ISO/IEC 27002: 8.1.3 Acceptable Use of Assets

HIPAA: Workstation Use 164.310(b) (R)

PCI-DSS: 12.3 Acceptable Usage

NIST: PL-4 Rules of Behavior

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 |  |
|  |  |  |  |  |