*Acceptable*

*Use of Assets Policy*

Table of Contents

[Purpose 1](#_Toc4059398)

[Scope 1](#_Toc4059399)

[Policy 1](#_Toc4059400)

[System Usage 1](#_Toc4059401)

[User IDs and Passwords 2](#_Toc4059402)

[Electronic Messaging 2](#_Toc4059403)

[Internet and Web Usage 3](#_Toc4059404)

[Data Storage 4](#_Toc4059405)

[System and Software Management 4](#_Toc4059406)

[Personal Equipment 5](#_Toc4059407)

[Physical Security 5](#_Toc4059408)

[System Ownership 5](#_Toc4059409)

[Telephones and Voice Mail 6](#_Toc4059410)

[Security Incident Reporting 6](#_Toc4059411)

[Violations 6](#_Toc4059412)

[Definitions 6](#_Toc4059413)

[References 7](#_Toc4059414)

[Related Documents 7](#_Toc4059415)

[Approval and Ownership 7](#_Toc4059416)

[Revision History 7](#_Toc4059417)

Purpose

This policy defines the acceptable use of all CompanyX (the “Company”) information system assets.

Scope

This policy applies to all employees and Third-Parties with access to CompanyX electronic information resources.

Policy

### System Usage

**Reasonable Personal Use Of Information Systems** - CompanyX allows computer users to make reasonable personal use of its electronic mail and other information systems. All such personal use must be consistent with conventional standards of ethical and polite conduct. For example, electronic mail must not be used to distribute or display messages or graphics which may be considered by some to be disruptive or offensive (such as sexual jokes or pornography).

**Use at your own Risk -** Users access the Internet with CompanyX facilities at their own risk. CompanyX 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 CompanyX systems is monitored and recorded. This information may include web sites visited, files downloaded, time spent on the Internet, and related information.

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

**Session Timeout** - Users must set the time frame for this period of no activity, at which point the contents of the screen are obscured, to 15 minutes or less. If sensitive information resides on a personal computer, the screen must immediately be protected with this access control package, or the machine turned off, whenever a worker leaves the location where the personal computer is in use.

### ****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** - CompanyX 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.

**Sharing Passwords** - Regardless of the circumstances, individual passwords must never be shared or revealed to anyone else besides the authorized user. Information Technology Department staff must never ask users to reveal their passwords.

**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 dial-up communications programs, Internet browsers, or related data communications software at any time.

**Suspected Password Disclosure** - Each user must immediately change his or her password if the password is suspected of being disclosed, or known to have been disclosed to an unauthorized party.

### Electronic Messaging

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

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

**No Guarantee of Message Privacy** - CompanyX cannot guarantee that electronic communications will be private. Users must be aware that electronic communications can, depending on the technology, be forwarded, intercepted, printed, and stored by others. Users must accordingly be careful about the topics covered in CompanyX electronic communications, and should not send a message discussing anything that they would not be comfortable reading about on the front page of their local newspaper.

**Outbound Electronic Mail Footer** - A footer prepared by the Legal Department must be automatically appended to all outbound electronic mail originating from CompanyX computers. This footer must make reference to the possibility that the message may contain confidential information, that it is for the use of the named recipients only, that the message has been logged for archival purposes, that the message may be reviewed by parties at CompanyX other than those named in the message header, and that the message does not necessarily constitute an official representation of CompanyX.

**Responding to Personal Information Requests** – CompanyX workers must never respond to electronic mail messages that request personal or sensitive company information, even from internal sources. The CompanyX 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.

**Responding to Offensive Messages** - Users must not to respond directly to the originator of offensive electronic mail messages, telephone calls, and/or other communications but instead report these instances to the Information Security Department.

**Harassing Of Offensive Materials** - CompanyX information systems are not intended to be used for, 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 CompanyX organizational changes or business policy matters. Sexual, ethnic, and racial harassment, including unwanted telephone calls, electronic mail, and internal mail, is strictly prohibited. Users must not use profanity, obscenities, or derogatory remarks in electronic mail messages discussing employees, customers, competitors, or others.

**Message Forwarding** - CompanyX Confidential information must not be forwarded to any party outside CompanyX without the prior approval. Messages sent by outside parties must not be forwarded to other Third-Parties unless the sender clearly intended this and such forwarding is necessary to accomplish an customary business objective. In all other cases, forwarding of messages sent by outsiders to other Third-Parties can be done only if the sender expressly agrees to this forwarding.

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

**Posting Sensitive Information** - Users must not post unencrypted CompanyX material on any publicly-accessible Internet computer that supports anonymous FTP or similar publicly-accessible services, unless the posting of these materials has been approved by the director of Public Relations.

**Disclosing Internal Information -** Users must not publicly disclose internal CompanyX by posting to any web site, including blogs, newsgroups, chat groups or social networking sites. Such information includes business prospects, products now in research and development, product performance analyses, product release dates, and internal information systems problems. Responses to specific customer electronic mail messages are exempted from this policy.

**Offensive Web Sites** - CompanyX 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. Users using CompanyX 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 CompanyX systems are permitted to visit that site. CompanyX 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 Security Department and must be for documented business purposes. Users are also prohibited from discussing specific CompanyX business within any personal home pages they may have established on these sites outside of CompanyX business hours.

### Data Storage

**Establishing Third-Party Networks** - Users must not establish any Third-Party information storage network that will handle CompanyX information (electronic bulletin boards, blogs, could storage) without the specific approval of the Information Security Department.

### System and Software Management

**Eradicating Computer Viruses** - Any user who suspects infection by a virus or malicious software must immediately call the corporate help desk, and make no attempt to eradicate the virus themselves without help from Information Technology Department.

**Trusted Software Scanning** - Users must not use any externally-provided software from a person or organization other than a known and trusted supplier unless the software has been scanned for malicious code and approved by the Information Security Department or a local Information Security Manager.

**Prohibition Against All Forms Of Adult Content** - All forms of adult content (pornography or what some would consider to be pornography) are prohibited on CompanyX computers and networks. This includes content obtained via web sites, email attachments, CD-ROMs, and file sharing networks.

**Unauthorized Software And Data Copies** - CompanyX strongly supports strict adherence to software vendors' license agreements and copyright holders' notices. If Internet users or other system users make unauthorized copies of software, the users are doing so on their own behalf, since all such copying is strictly forbidden by CompanyX. Likewise, CompanyX allows reproduction of copyrighted material only to the extent legally considered "fair use" or with the permission of either the author or publisher.

**Involvement With Computer Viruses** - Users must not intentionally write, generate, compile, copy, collect, propagate, execute, or attempt to introduce any computer code designed to self-replicate, damage, or otherwise hinder the performance of any CompanyX computer or network.

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

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

**Current Virus Software**- Every CompanyX worker who examines, processes, or stores CompanyX 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 Security Department.

**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 Security Manager.

**Sharing A Personal Computer With Other People Prohibited** - Users must not share their personal computer, if it is used for CompanyX business, with any other person.

**Accepting Security Assistance From Outsiders** - Users must not accept any form of assistance to improve the security of their computers without first having the provider of this assistance approved by the CompanyX Information Security Department. This means that users must not accept offers of free consulting services, must not download free security software via the Internet, and must not employ free security posture evaluation web pages, unless the specific provider of the assistance has been previously approved.

### Physical Security

**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, workstation, or terminal unattended without logging out or invoking a password-protected screen saver.

**Positioning Display Screens** - The display screens for all personal computers used to handle sensitive or valuable data must be positioned such that the information cannot be readily viewed through a window, by persons walking in a hallway, or by persons waiting in reception and related areas. Care must also be taken to position keyboards so that unauthorized persons cannot readily see workers enter passwords, encryption keys, and other security-related parameters.

**Locking Sensitive Information** - When not being used by authorized workers, or when not clearly visible in an area where authorized persons are working, all hardcopy sensitive information must be locked in file cabinets, desks, safes, or other furniture. When not being used, or when not in a clearly visible and attended area, all computer storage media containing sensitive information must be locked in similar enclosures.

### System Ownership

**Personal Equipment Approval** - Users must not bring their own computers, computer peripherals, or computer software into CompanyX facilities without prior authorization from their department head. Users must not use their own personal computers for production CompanyX business unless these systems have been evaluated and approved by the Information Security Department.

**Custodians For Equipment** - The primary user of a personal computer is considered a Custodian for the equipment. If the equipment has been damaged, lost, stolen, borrowed, or is otherwise unavailable for normal business activities, a Custodian must promptly inform the involved department manager. With the exception of portable machines, personal computer equipment must not be moved or relocated without the knowledge and approval of the involved department manager.

**Property Pass** - Personal computers, portable computers and related information systems equipment must not leave CompanyX offices unless accompanied by a property pass signed by a department manager.

### Telephones and Voice Mail

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

**Use of VOIP on Personal Computers** - CompanyX workers must not make telephone calls that communicate confidential or secret information using softphones that support voice over IP on their personal computers.

### ****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 Security Manager. Examples of these events include:

* Any unauthorized use of CompanyX 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 CompanyX information to unauthorized Third-Parties.

Violations

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

Any employee or contractor who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

Confidential Information (Sensitive Information) – Any CompanyX 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 CompanyX from a Third-Party under a non-disclosure agreement

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

Mobile Computing Devices - Mobile computing assets include, but are not limited to: laptop, notebook, tablet, desktop computers, all personal wireless-enabled devices, including pagers, cellular phones, mobile email devices, PDAs and other hybrid devices, and all portable storage media, including flash drives, smart cards, tokens, etc.

**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.

**Third-Party –** Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002: 8.1.3 Acceptable Use of Assets

PCI-DSS: 12.3 Acceptable Usage

NIST: PL-4 Rules of Behavior

US-CSF: PR.AT-1: All users are informed and trained

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 | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |