Information Security Policies

Sample Internet Acceptable Use Policy

Policy #	IS-01	Effective Date	MM/DD/YYYY	Email	contact@companyx.com
Version	1.0	Contact	Policy Contact	Phone	888.123.4567

Table of Contents

Purpose....1
Scope....1
Policy....1
Violations....3
Definitions....3
References....3
Related Documents....3
Approval and Ownership....3
Revision History....3

PURPOSE

This policy establishes the minimum requirements and responsibilities for the secure connection and use of the internet and other public networks by Company X employees and contractors.

SCOPE

This policy applies to all workers, employees, contractors, consultants, temporaries, and volunteers, who use the Internet with Company X computing or networking resources.

POLICY

Required Approval

Prior Management Approval - Company X users must not access the internet without a proper understanding of the associated personal and business risks. In order to receive Internet access privileges, all workers must complete the Company X computer-based training information security course then pass the accompanying test. Access to the Internet, aside from electronic mail, will be provided to only those workers who have a legitimate business need for such access. The ability to access the Internet and engage in other Internet activities is not a fringe benefit to which all workers are entitled. If a worker does not have sufficient Internet access, but needs access for a particular project, he or she can use the special shared systems established by Company X management.

Information Integrity

Information Reliability - All information acquired from the Internet must be considered suspect until confirmed by separate information from another source. Before using free

Internet-supplied information for business decision-making purposes, workers must corroborate the information by consulting other sources.

Virus Checking - All non-text files downloaded from non-Company X sources through the Internet must be screened with current virus detection software prior to being used. Whenever an external provider of the software is not trusted, downloaded software must be tested on a stand-alone, non-production machine that has been recently backed up. Downloaded files must be decrypted and decompressed before being screened for viruses. The use of digital signatures to verify that a file has not been altered by unauthorized parties is recommended, but this does not assure freedom from viruses, Trojan horses, and other problems.

Software Downloading - Company X has implemented an automatic software distribution system to install the latest release of licensed software on Company X computers. A separate system is used to automatically trace all software resident on these same systems. As discussed in the Personal Computer Security Policy, workers must not install software on their Company X-supplied computers, whether the software was downloaded from the Internet or procured elsewhere.

Push Technology - Automatic updating of software or information on Company X computers through background push Internet technology is prohibited unless the involved vendor's system has been tested and approved by the Internet group within the Information Systems department.

Spoofing Users - Before workers release any internal Company X information, enter into any contracts, or order any products through public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed through digital signatures or digital certificates, but in cases where these are not available, other means such as letters of credit, third-party references, and telephone conversations may be used.

User Anonymity - Misrepresenting, obscuring, suppressing, or replacing a user's identity on the Internet or any Company X electronic communications system is forbidden. The user name, electronic mail address, organizational affiliation, and related information included with messages or postings must reflect the actual originator of the messages or postings. If users have a need to employ remailers or other anonymous facilities, they must do so on their own time, with their own information systems and Internet service provider accounts. Use of anonymous FTP logons, anonymous UUCP logons, HTTP or web browsing, and other access methods established with the expectation that users would be anonymous are permissible.

Electronic Mail Attachments - Workers must not open electronic mail attachments unless they were expected from a trusted sender. When they are expected from a known and trusted sender, attachments must be scanned with a virus package prior to being opened.

Responding to Information Requests – Workers must never respond to unsolicited requests for personal information, including passwords or credit card numbers, from an electronic mail message. Any such message should be immediately reported to the Information Security department.

Web Page Changes - Workers must not establish new Internet pages dealing with Company X business, or make modifications to existing web pages dealing with Company X business, unless they have obtained the approval of the Internet management committee.

Modifications include the addition of links to other sites, updating the information displayed, and altering the graphic layout of a page. This committee must ensure that all posted material has a consistent and polished appearance, is aligned with business goals, and is protected with adequate security measures.

Web Page Archives - Every version of the Company X Internet site and commerce site files must be securely archived in two physically separated locations. The Internet management committee will designate a web master who will keep this archive and provide copies of historical pages on demand.

Information Confidentiality

Information Exchange - Company X software, documentation, and all other types of internal information must not be sold or otherwise transferred to any non-Company X party for any purposes other than business purposes expressly authorized by management. Exchanges of software or data between Company X and any third party must not proceed unless a written agreement has been signed. Such an agreement must specify the terms of the exchange, and the ways that the software or data is to be handled and protected. Regular business practices, such as shipment of a product in response to a customer purchase order, need not involve such a specific agreement since the terms and conditions are implied.

Posting Materials - Workers must not post unencrypted Company X 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. Company X internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate business need to know the involved information.

Message Interception - Company X secret, proprietary, or private information must not be sent over the Internet unless it has been encrypted by approved methods. Unless specifically known to be in the public domain, source code must always be encrypted before being sent over the Internet. For the same reasons, Internet telephone services must not be used for Company X business unless the connection is known to be encrypted.

Security Parameters - Unless a connection is known to be encrypted, credit card numbers, telephone calling card numbers, fixed logon passwords, and other security parameters that can be used to gain access to goods or services, must not be sent over the Internet in readable form. Encryption processes are permissible if they are approved by the corporate Information Security manager.

Public Representations

External Representations - Workers may indicate their affiliation with Company X in mailing lists, chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for example through an electronic mail address. In either case, whenever workers provide an affiliation, unless they have been expressly designated as a spokes-person of Company X, they also must clearly indicate the opinions expressed are their own, and not necessarily those of Company X. If an affiliation with Company X is provided, political advocacy statements and product or service endorsements also are prohibited unless they have been previously cleared by the director of Public Relations. With the exception of ordinary marketing and customer service activities, all representations on behalf of Company X must be cleared by the director of Public Relations.

Private Email Addresses – Workers posting information on any publicly available web site must not include their personal Company X electronic mail address. These postings are used to generate SPAM against company X. Company X issues separate email addresses for specific public postings. Users who require the external posting of their personal email address must request permission from their manager or the director of Public Relations..

Appropriate Behavior - Whenever any affiliation with Company X is included with an Internet message or posting, written attacks are strictly prohibited. Workers must not make threats against another user or organization over the Internet. All Internet messages intended to harass, annoy, or alarm another person are similarly prohibited.

Removal Of Postings - Those messages sent to Internet discussion groups, electronic bulletin boards, or other public forums, that include an implied or explicit affiliation with Company X, may be removed if management deems them to be inconsistent with Company X business interests or existing company policy. Messages in this category include political statements, religious statements, cursing or other foul language, and statements viewed as harassing others based on race, creed, color, age, sex, physical handicap, or sexual orientation. The decision to remove electronic mail must be made by the corporate Information Security manager or the director of Human Resources. When practical and feasible, individuals responsible for the message will be informed of the decision and given the opportunity to remove the message themselves.

Disclosing Internal Information - Workers must not publicly disclose internal Company X information through the Internet that may adversely affect the Company X stock price, customer relations, or public image unless the approval of the director of Public Relations or a member of the top management team has been obtained. 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.

Inadvertent Disclosure - Care must be taken to properly structure comments and questions posted to mailing lists, public news groups, Usenet, and related public postings on the Internet. Before posting any material, workers must consider whether the posting could put Company X at a significant competitive disadvantage or whether the material could cause public relations problems. Workers should keep in mind that several separate pieces of information can be pieced together by a competitor to form a picture revealing confidential information that then could be used against Company X. Workers must never post on the Internet the specific computer or network products employed by Company X.

Intellectual Property Rights

Copyrights - When at work, or when Company X computing or networking resources are employed, copying of software in a manner that is not consistent with the vendor's license is strictly forbidden. Off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Company X work, and are therefore prohibited. The reproduction, forwarding, or in any other way republishing or redistribution of words, graphics, or other copyrighted materials must be done only with the permission of the author or Owner. Workers must assume that all materials on the Internet are copyrighted unless specific notice states otherwise. When information from the Internet is integrated into internal reports or used for other purposes, all material must include labels such as "copyright, all rights reserved" and specifics about the source of the information.

Publicly-Writable Directories - All publicly-writable directories on Company X Internet-connected computers must be reviewed and cleared each evening. Workers using Company X computers must not be involved in any way with the exchange of pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material.

Access Control

Inbound User Authentication - All users wishing to establish a real-time connection with Company X internal computers through the Internet must employ a virtual private network (VPN) product approved by the Information Security department that can encrypt all traffic exchanged. These VPN products also must authenticate remote users at a firewall before permitting access to the Company X internal network. This authentication process must be achieved through a dynamic password system approved by the corporate Information Security manager. Examples of approved technology include hand-held smart cards with dynamic passwords and user-transparent challenge and response systems. Designated public systems do not need user authentication processes because anonymous interactions are expected.

Remote Machine Security - Workers who have not installed required software patches or upgrades, or whose systems are virus-infested must be disconnected automatically from the Company X network until they have reestablished a secure computing environment. The computers used by all workers employing VPN technology must be remotely scanned automatically to determine that the software is current and that the system has been properly secured.

Restriction Of Third-Party Access - Inbound Internet access privileges must not be granted to third-party vendors, contractors, consultants, temporaries, outsourcing organization personnel or other third parties unless the relevant system manager determines that these individuals have a legitimate business need for such access. These privileges must be enabled only for specific individuals and only for the time period required to accomplish approved tasks.

Browser User Authentication - Workers must not save fixed passwords in their web browsers or electronic mail clients. These fixed passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if a boot password must be provided each time the computer is powered up, and if a screen saver password must be provided each time the system is inactive for a specified period of time. Company X computer users must refuse all offers by software to place a cookie on their computer so that they can automatically log on the next time that they visit a particular Internet site. Cookies that serve other purposes are permissible.

Data Aggregators - Workers must not provide their Internet user IDs and passwords to data aggregators, data summarization and formatting services, or any other third parties.

Internet Service Providers - With the exception of telecommuters and mobile computer users, workers must not employ Internet service provider accounts and dial-up lines to access the Internet with Company X computers. All Internet activity must pass through Company X firewalls so that access controls and related security mechanisms can be applied. Users must employ their Company X electronic mail address for Internet electronic mail. Use of a personal electronic mail address for this purpose is prohibited.

Establishing Network Connections - Unless the prior approval of the manager of Telecommunications Services has been obtained, workers must not establish Internet or other external network connections that could permit non-Company X users to gain access to Company X systems and information. These connections include the establishment of multi-computer file systems, Internet pages, Internet commerce systems, and FTP servers.

Establishing New Business Channels - Unless the vice president of Information Systems, the vice president of Marketing, and the chief legal counsel have approved in advance, workers must not use new or existing Internet connections to establish new business channels. These channels include electronic data interchange arrangements, electronic malls with online shopping, and online database services.

Conducting Business Over The Internet - Unless advance approval of the Purchasing department has been obtained, Company X workers must not purchase any goods or services through the Internet if these goods or services are offered by a business based in, or operating out of, a foreign country.

Personal Use

Personal Use - Workers who have been granted Internet access and who wish to explore the Internet for personal purposes must do so on personal rather than company time. Games, news groups, and other non-business activities must be performed on personal, not company time. Use of Company X computing resources for these personal purposes is permissible as long as the incremental cost of the usage is negligible, no Company X business activity is preempted by the personal use, and the usage is not likely to cause either a hostile working environment or a poor behavioral example. Workers must not employ the Internet or other internal information systems in such a way that the productivity of other workers is eroded. Examples of this include chain letters and broadcast charitable solicitations. Company X computing resources must not be resold to other parties or used for any personal business purposes such as running a consulting business on off-hours.

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.

Use of “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. Company X reserves the right to block access to these or other web sites. Workers are also prohibited from discussing specific company X business within any personal home pages they may have established on this sites outside of Company X business hours.

Privacy Expectations

No Default Protection - Workers using Company X information systems or the Internet must realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers must not send information over the Internet if they consider it to be confidential or private.

Management Review - At any time and without prior notice, Company X management reserves the right to examine electronic mail messages, files on personal computers, web browser cache files, web browser bookmarks, logs of web sites visited, computer system configurations, and other information stored on or passing through Company X computers.

Logging - Company X routinely logs the web sites visited, files downloaded, time spent on the Internet, and related information. Department managers receive reports of such information and use it to determine what types of Internet usage are appropriate for their department's business activities.

Junk Electronic Mail - Users must not use Company X computer systems for the transmission of unsolicited bulk electronic mail advertisements or commercial messages that are likely to trigger complaints from the recipients. These prohibited messages include a wide variety of unsolicited promotions and solicitations such as chain letters, pyramid schemes, and direct marketing pitches. When workers receive unwanted and unsolicited electronic mail, they must refrain from responding directly to the sender. They must forward the message to the electronic mail administrator at Company X who then can take steps to prevent further transmissions.

Reporting Security Problems

Notification Process - If sensitive Company X information is lost, disclosed to unauthorized parties, or suspected of either, the Information Security manager must be notified immediately. If any unauthorized use of Company X information systems has or is suspected of taking place, the corporate Information Security manager must be notified immediately. Whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the corporate Information Security manager must be notified immediately. All unusual systems behavior, such as missing files, frequent system crashes, and misrouted messages must be immediately reported to the help desk. The specifics of security problems must not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports - Workers in receipt of information about system vulnerabilities must forward it to the corporate Information Security manager, who then will determine what if any action is appropriate. Workers must not personally redistribute system vulnerability information to other users.

Testing Controls - Workers must not test or probe security mechanisms at either Company X or other Internet sites unless they have obtained written permission from the corporate Information Security manager. The possession or the usage of tools for detecting information system vulnerabilities, or tools for compromising information security mechanisms, are prohibited without the advance permission of the corporate Information Security manager.

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.

Any employee or partner 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 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.

Electronic Messaging System – Any device or application that will provide the capability of exchanging digital communication between two or more parties. Examples are electronic messaging, instant messaging, and text messaging.

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.

Objectionable Information or Material – Anything that is considered offensive, defamatory, obscene, or harassing, including, but not limited to, sexual images, jokes and comments, racial or gender-specific slurs, comments, images or jokes, or any other comments, jokes, or images that would be expected to offend someone based on their physical or mental disability, age, religion, marital status, sexual orientation, political beliefs, veteran status, national origin, or ancestry, or any other category protected by national or international, federal, regional, provincial, state, or local laws.

Partner – 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

ISO 27002 - 7.1.3 Acceptable use of assets

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	