Internet Security Policy

INTRODUCTION

Opportunities & Risks

The wide array of new resources, new services, and interconnectivity available via the Internet all introduce new opportunities and new risks. In response to the risks, this policy describes Company X's official policy regarding Internet security.

Applicability

This policy applies to all workers (employees, contractors, consultants, temporaries, etc.) who use the Internet with Company X computing or networking resources, as well as those who represent themselves as being connected--in one way or another--with Company X. All Internet users are expected to be familiar with and comply with this policy. Questions about the policy should be directed to the Information Security Coordinator. Violations of this policy can lead to revocation of system privileges and/or disciplinary action up to and including termination.

Prior Management Approval

Access to the Internet (aside from electronic mail) will be provided to only those employees who have a legitimate need for such access. The ability to surf the web 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 such access for a particular project, he or she can use the special shared systems found in the Corporate Library. In order to receive Internet access privileges, all workers must first attend an information security training course.

INFORMATION INTEGRITY

Information Reliability

All information taken off the Internet should be considered suspect until confirmed by separate information from another source. There is no quality control process on the Internet, and a considerable amount of its information is outdated and inaccurate, and in some instances even deliberately misleading. Accordingly, 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 (databases, software object code, spreadsheets, formatted word processing package files, etc.) downloaded from non-Company X sources via the

Internet must be screened with virus detection software prior to being used. Whenever an external provider of the software is not trusted, down-loaded software should be tested on a stand-alone non-production machine that has been recently backed-up. If this software contains a virus, worm, or Trojan horse, then the damage will be restricted to the involved machine. Downloaded files must be decrypted and decompressed before being screened for viruses. Separately, the use of digital signatures to verify that unauthorized parties have not altered a file is recommended, but this does not assure freedom from viruses.

Push Technology

Automatic updating of software or information on Company X computers via background "push" Internet technology is prohibited unless the involved vendor's system has first been tested and approved by the Internet Group within the Information Systems Department. While powerful and useful, this new technology could be used to spread viruses, and cause other operational problems such as system unavailability.

Spoofing Users

Unless tools like digital signatures and digital certificates are employed, it is relatively easy to spoof the identity of another user on the Internet. Before workers release any internal Company X information, enter into any contracts, or order any products via public networks, the identity of the individuals and organizations contacted must be confirmed. Identity confirmation is ideally performed via 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 with their own Internet access accounts. Use of anonymous FTP log-ins, anonymous UUCP log-ins, HTTP (web) browsing, and other access methods established with the expectation that users would be anonymous are permissible.

Web Page Changes

Workers may not establish new Internet web pages dealing with Company X business, or make modifications to existing web pages dealing with Company X business, unless they have first obtained the approval of the Internet

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

INFORMATION CONFIDENTIALITY

Information Exchange

In keeping with the confidentiality agreements signed by all workers, 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 and/or data between Company X and any third party may not proceed unless a written agreement has first been signed. Such an agreement must specify the terms of the exchange, as well as the ways in which the software and/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 (software, internal memos, policies, etc.) on any publicly accessible Internet computer, which supports anonymous FTP or similar publicly accessible services, unless the Director of Public Relations has first approved the posting of these materials. In more general terms, Company X internal information must not be placed in any computer unless the persons who have access to that computer have a legitimate need-to-know the involved information.

Message Interception

Wiretapping and other types of message interception are straightforward and frequently encountered on the Internet. Accordingly, Company X secret, proprietary, or private information must not be sent over the Internet unless it has first 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: Credit card numbers, telephone calling card numbers, fixed login 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. The SSL or SET encryption processes are both acceptable Internet encryption standards for the protection of security parameters. Other encryption processes, such as

PGP, are permissible if the Corporate Manager of Information Security approves them.

PUBLIC REPRESENTATIONS

External Representations: Workers may indicate their affiliation with Company X in mailing lists (listservs), chat sessions, and other offerings on the Internet. This may be done by explicitly adding certain words, or it may be implied, for instance via an electronic mail address. In both case, whenever workers provide an affiliation, they must also clearly indicate the opinions expressed are their own, and not necessarily those of Company X. Likewise, if an affiliation with Company X is provided, political advocacy statements and product/service endorsements are also prohibited unless the Director of Public Relations has previously cleared them. With the exception of ordinary marketing and customer service activities, the Director of Public Relations must first clear all representations on behalf of the company.

Appropriate Behavior: To avoid libel, defamation of character, and other legal problems, whenever any affiliation with Company X is included with an Internet message or posting, "flaming" or similar written attacks are strictly prohibited. Likewise, 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, which include an implied or explicit affiliation with Company X, may be removed if management deems them to be inconsistent with Company X's business interests or existing Company policy. Messages in this category include: (a) political statements, (b) religious statements, (c) cursing or other foul language, and (d) 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 Manager of Information Security 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(s) themselves.

Disclosing Internal Information: Workers must not publicly disclose internal Company X information via the Internet that may adversely affect Company X's 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 first been obtained. Such information includes business prospects, products now in

research and development, product performance analyses, product release dates, internal information systems problems, and the like. 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 (listservs), 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 which could then be used against Company X. Although it may seem to be different than the prevailing Internet culture of openness, to avoid this mosaic picture problem, workers should be reserved rather than forthcoming with internal Company X information.

INTELLECTUAL PROPERTY RIGHTS

Copyrights: Company X strongly supports strict adherence to software vendors' license agreements. 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. Likewise, off-hours participation in pirate software bulletin boards and similar activities represent a conflict of interest with Company X work, and are therefore prohibited. Similarly, the reproduction, forwarding, or in any other way republishing or redistributing words, graphics, or other materials must be done only with the permission of the author/owner. Workers should 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" as well as specifics about the source of the information (author names, URLs, dates, etc.).

Publicly Writable Directories: All publicly writable directories on Company X Internet-connected computers will be reviewed and cleared each evening. This process is necessary to prevent the anonymous exchange of information inconsistent with Company X's business. Examples include pirated software, purloined passwords, stolen credit card numbers, and inappropriate written or graphic material (for instance, pornography). Workers using Company X computers must not be involved in any way with the exchange of the material described in the last sentence.

ACCESS CONTROL

Inbound User Authentication: All users wishing to establish a real-time connection with Company X internal computers via the Internet must authenticate themselves at a firewall before gaining access to Company X's internal network. This authentication process must be achieved via a dynamic password system approved by the Corporate Manager of Information Security. Examples of approved technology include hand-held smart cards with dynamic passwords and user-transparent challenge/response systems. These systems will prevent intruders from guessing fixed passwords or from replaying a fixed password captured via a "sniffer attack" (wiretap). Designated "public" systems (anonymous ftp, web surfing, etc.) do not need user authentication processes because anonymous interactions are expected.

Browser User Authentication: Users must not save fixed passwords in their web browsers or electronic mail clients because this may allow anybody who has physical access to their workstations to both access the Internet with their identities, as well as read and send their electronic mail. Instead, these fixed passwords must be provided each time that a browser or electronic mail client is invoked. Browser passwords may be saved if and only 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.

Internet Service Providers: With the exception of telecommuters and mobile computer users, workers must not employ Internet Service Provider (ISP) accounts and dial-up lines to access the Internet with Company X computers. Instead, all Internet activity must pass through Company X firewalls so that access controls and related security mechanisms can be applied.

Establishing Network Connections: Unless the prior approval of the Manager of Telecommunications Services has been obtained, workers may not establish Internet or other external network connections that could allow non-Company X users to gain access to Company X systems and information. These connections include the establishment of multi-computer file systems (like Sun's NIS), Internet web pages, Internet commerce systems, ftp servers, and the like.

Establishing New Business Channels: Unless the VP of Information Systems, the VP of Marketing, and the Chief Legal Counsel have all approved in advance, workers are prohibited from using new or existing Internet connections to establish new business channels. These channels include electronic data

interchange (EDI) arrangements, electronic malls with on-line shopping, on-line database services, etc.

PERSONAL USE

Personal Use: Company X management encourages workers who have been granted Internet access to explore the Internet, but if this exploration is for personal purposes, it must be done on personal, not company time. Likewise, 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 so long as the incremental cost of the usage is negligible, and so long as no Company X business activity is preempted by the personal use. Workers must not employ the Internet or other internal information systems in such a way that the productivity of other workers is eroded; examples include chain letters and broadcast charitable solicitations.

Blocking Sites: Company X firewalls routinely prevent users from connecting with certain non-business web sites. Workers using Company X computers who discover they have connected with a web site that contains sexually explicit, racist, violent, or other potentially offensive material must immediately disconnect from that site. 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.

PRIVACY EXPECTATIONS

No Default Protection: Workers using Company X information systems and/or the Internet should realize that their communications are not automatically protected from viewing by third parties. Unless encryption is used, workers should 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, and other information stored on or passing through Company X computers. Such management access assures compliance with internal policies, assists with internal investigations, and assists with the management of Company X information systems.

Logging: Company X routinely logs 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 Email: When workers receive unwanted and unsolicited email (also known as spam), they must refrain from responding directly to the sender. Instead, they should forward the message to the email administrator at Company X who can then take steps to prevent further transmissions. To respond to the sender would be indicate that the user-ID is monitored regularly, and this would then invite further junk email.

REPORTING SECURITY PROBLEMS

Notification Process: If sensitive Company X information is lost, disclosed to unauthorized parties, or suspected of being lost or disclosed to unauthorized parties, the Corporate Manager of Information Security must be notified immediately. If any unauthorized use of Company X's information systems has taken place, or is suspected of taking place, the Corporate Manager of Information Security must likewise be notified immediately. Similarly, whenever passwords or other system access control mechanisms are lost, stolen, or disclosed, or are suspected of being lost, stolen, or disclosed, the Corporate Manager of Information Security must be notified immediately. Because it may indicate a computer virus infection or similar security problem, all unusual systems behavior, such as missing files, frequent system crashes, misrouted messages, and the like must also be immediately reported. The specifics of security problems should not be discussed widely but should instead be shared on a need-to-know basis.

False Security Reports: The Internet has been plagued with hoaxes alleging various security problems. Many of these hoaxes take the form of chain letters, which request that the receiving party send the message to other people. Workers in receipt of information about system vulnerabilities should forward it to the Corporate Manager of Information Security, who will then determine what if any action is appropriate. Workers must not personally redistribute system vulnerability information.

Testing Controls: Workers must not "test the doors" (probe) security mechanisms at either Company X or other Internet sites unless they have first obtained permission from the Corporate Manager of Information Security. If workers probe security mechanisms, alarms will be triggered and resources will needlessly be spent tracking the activity. Likewise, both the possession and the usage of tools for cracking information security (such as SATAN) are prohibited

without the advance permission of the Corporate Manager of Information Security.