|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information Exchange Security Policy | | | | | |
| Policy # | CPL-05-03 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457847854)

[Scope 1](#_Toc457847855)

[Policy 2](#_Toc457847856)

[Disclosure Restrictions 2](#_Toc457847857)

[Public Information Disclosures 2](#_Toc457847858)

[Exchange Agreements 2](#_Toc457847859)

[Physical Transit Controls 3](#_Toc457847860)

[Confidential Information Removal 3](#_Toc457847861)

[Electronic Transmission 3](#_Toc457847862)

[Electronic Mail 4](#_Toc457847863)

[Travel Considerations 4](#_Toc457847864)

[Faxing Information 4](#_Toc457847865)

[Customer Communications 5](#_Toc457847866)

[Business Information Systems 5](#_Toc457847867)

[Internet and Intranet 6](#_Toc457847868)

[Intranet Content 6](#_Toc457847869)

[Web Site Security 6](#_Toc457847870)

[Public Information 7](#_Toc457847871)

[Violations 7](#_Toc457847872)

[Definitions 7](#_Toc457847873)

[References 8](#_Toc457847874)

[Related Documents 8](#_Toc457847875)

[Approval and Ownership 8](#_Toc457847876)

[Revision History 8](#_Toc457847877)

Purpose

This policy defines controls for the proper disposal of all Company X sensitive information, either in paper or electronic format.

Scope

This policy applies to all Company X computer systems and facilities, including those managed for Company X customers. This policy applies to all employees, partners and third-parties with access to Company X information assets in digital or hardcopy form.

Policy

### ****Disclosure Restrictions****

**External Information Requests** - All requests from a third party for internal information that is not classified as PUBLIC must be approved by both the Information Owner and the Company X corporate counsel, who must each be given five business days to evaluate the merits of the request.

**Information Transfer To Third Parties** - 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 those expressly authorized by management.

**Requests For Organization Information** - Unless authorized by management, all requests for information about Company X and its business activities including, but not limited to, questionnaires, surveys, and newspaper interviews, must be referred to the Public Relations Department.

### ****Public Information Disclosures****

**Public Representation Approval** - All public representations including, but not limited to, media advertisements, Internet home pages, electronic bulletin board postings, and voice mail broadcast messages, must be issued or approved by the Public Relations Department.

**Information Released To The Public — Contact Name** - Information generated by Company X and released to the public must be accompanied by the name of a designated staff member acting as the single recognized official source and point-of-contact.

**Release Of Organization Information** - Permission to disclose any internal Company X information to the news media or to other third parties must be obtained from Company X senior management prior to release.

**Information Released To The Public — Authorization** - All internal Company X information to be released to the public must have first been reviewed by management according to an established and documented process.

### ****Exchange Agreements****

**Software And Data Exchange Agreements** - Exchanges of in-house software or internal information between Company X and any third party must be accompanied by a written agreement that specifies the terms of the exchange, and the manner in which the software or information is to be handled and protected.

**Third-Party Software Agreements** - All software developed by Company X for use by prospects, customers, business partners, and others, must be distributed only after the recipients have signed an agreement stating they will not disassemble, reverse engineer, modify, or otherwise use the programs except as agreed with Company X.

**Online Contracts By Exchange Of Paper And Signatures** - Whenever third parties accept an online offer made by Company X, they must provide paper-based, hand-rendered signatures by regular mail or courier.

**Identity Validation Of External Parties** - 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 through digital certificates, letters of credit, third-party references, or telephone conversations.

### ****Physical Transit Controls****

**Delivering Sensitive Computer Output** - Confidential computer system hardcopy output must be personally delivered to the designated recipients and never delivered to an unattended desk, or left out in the open in an unoccupied office.

**Using Couriers** - Private, Confidential, or Confidential information in hardcopy form that is sent through commercial courier must always be tracked with a weigh bill number and must always be marked recipient “signature required.”

**Sending Confidential Information – Mail Packaging** - If private or confidential information is sent through internal mail, external mail, or by courier, it must be enclosed in two envelopes or containers with the outside envelope or container providing no indication of the sensitivity of the information contained therein and the inside sealed and opaque envelope or container labeled “Private,” “Confidential,” or “Confidential.”

**Sending Confidential Information - Packaging** - Confidential information must be shipped or sent through internal or external mails in a sealed opaque envelope marked “To Be Opened By Addressee Only,” which is enclosed in a plain outer envelope that does not indicate the sensitivity of the contents.

**Sending Confidential Information – Transport** - Private and confidential information must be shipped or sent through internal or external mails in a sealed opaque envelope marked “To Be Opened By Addressee Only.”

**Sending Confidential Hardcopy Information** - Confidential information in hardcopy form must be sent by trusted courier or registered mail.

### ****Confidential Information Removal****

**Confidential Information Leaving Offices** - Confidential Company X information, no matter what form it happens to take, must not leave Company X offices unless the approval of the Information Security Manager has first been obtained.

**Sensitive Information Removal Log** - All sensitive information removed from Company X premises must be logged with a record of the date, the information involved, and the persons possessing the information.

**Delivery Of Confidential Information** - All deliveries of confidential information must be conducted such that the recipient formally acknowledges that the information has been received.

### ****Electronic Transmission****

**Transferring Sensitive Information** - Before any Company X Confidential or private information may be transferred from one computer to another, the worker making the transfer must ensure that access controls on the destination computer are commensurate with access controls on the originating computer.

**Wireless Transmissions Of Confidential Information** - Wireless technology must never be used for the transmission of unencrypted confidential information.

**Third-Party Delivery Of Confidential Information** - Unencrypted confidential information must not be sent through any third parties including, but not limited to, couriers, postal services, telephone companies, and Internet service providers.

**Public Network Data Transmission** - Strong cryptography and security protocols such as SSL/TLS or IPSEC must be implemented to safeguard confidential Company X information during transmission over open, public networks.

**Confidential Data Electronic Transmission** - All Company X confidential data transmitted over any communication network must be encrypted.

**Confidential Information Encryption** - All computerized confidential information must be encrypted, with tools approved by the Information Security Department, when not in active use for authorized business purposes.

### ****Electronic Mail****

**Electronic Mail Encryption** - All sensitive information including, but not limited to electronic health information (EPHI) must be encrypted when transmitted through electronic mail.

**Electronic Mail Approval** - Unencrypted sensitive or confidential information must not be sent by electronic mail unless a vice president specifically authorizes each occurrence.

**Electronic Mail Addresses** - Workers must not employ any electronic mail addresses other than official Company X electronic mail addresses for all company business matters.

### ****Travel Considerations****

**International Travel - Special Travel Laptops Required** - All Company X employees traveling with Confidential information must only use special “travel” laptops issued by the Information Technology department.  These special devices are stripped of all non-essential information and must employ both full-disk encryption and two-factor authentication.

**Traveling With Confidential Information** - Workers must not travel on public transportation when in the possession of confidential Company X information unless specific management approval has been obtained.

**International Transport Of Confidential Information — Security** - Whenever confidential information is carried by a Company X worker into a foreign country, the information must either be stored in some inaccessible form or must remain in the worker’s possession at all times.

**International Transport Of Confidential Information — Authorization** - Company X workers must not take confidential Company X information into another country unless advance permission has been obtained from the Information Security Manager.

### ****Faxing Information****

**Fax Cover Sheet Notice** - All outgoing Company X faxes must include a cover sheet that includes wording approved by the Legal Department.

**Fax Logs** - Logs reflecting the involved phone numbers and the number of pages for all inbound and outbound fax transmissions must be retained for one year.

**Faxing Sensitive Information — Notification** - If sensitive information is to be sent by fax, the recipient must have been notified of the time when it will be transmitted, and also have agreed that an authorized person will be present at the destination machine when the material is sent. An exception to this policy is permitted when the destination fax machine is physically or logically restricted such that persons who are not authorized to see the material being faxed may not enter the immediate area or otherwise gain access to faxes received.

**Faxing Sensitive Information — Human Presence** - Sensitive materials must not be faxed unless the sender has immediately beforehand confirmed that an authorized staff member is on hand to properly handle the materials at the receiving machine. When the transmission is complete, the staff member at the receiving end must confirm to the sender that a certain number of pages were received. An exception is allowed if the receiving machine is in a locked room accessible only to authorized personnel, or if a password-protected fax mailbox is used to restrict unauthorized release of faxed materials.

**Faxing Sensitive Information — Intermediaries** - Sensitive Company X information must not be faxed through un-trusted intermediaries including, but not limited to, hotel staff, airport office services staff, and rented mailbox store staff.

**Faxing Sensitive Information — Dual Cover Sheet** - When sensitive information must be faxed, a cover sheet must be sent and acknowledged by the recipient, after which the sensitive information may be sent through a second call.

**Faxing Sensitive Information — Physical Security** - Confidential information must not be sent to an unattended fax machine unless the destination machine is in a locked room for which the keys are possessed only by people authorized to receive the information.

**Faxing Sensitive Information - Annual Inventory of FAX numbers** - Company X must maintain an inventory of all outgoing FAX numbers and the associated organization designated to receive sensitive information.  The list of numbers must be updated and verified annually.  The list must be distributed to all personnel responsible for transmitting sensitive data.

### ****Customer Communications****

**Electronic Mail Distributions** - Company X must receive a positive confirmation through an opt-in process for anyone who is placed on an electronic mail distribution list.

**Customer Status Notifications Sent Via Electronic Mail** - Company X must not use electronic mail as the sole source of notification for changes or updates to customer account features. Any customer notifications sent via electronic mail will include instructions for validating the authenticity of the message.

**Electronic Marketing Material Source** - All marketing materials sent through electronic mail must include an accurate return address and must provide clear and explicit instructions permitting recipients to quickly be removed from the distribution list.

### Business Information Systems

**Intermediate Products Containing Sensitive Information** - If a copy machine jams or malfunctions when workers are making copies of confidential information, they must not leave the machine until all copies of the information are removed from the machine or destroyed beyond recognition.

**Distribution Of Marketing Materials** - Workers must not use facsimile machines, electronic mail, auto-dialer robot voice systems, or any other electronic communications systems for the distribution of unsolicited advertising material.

**Recording Video Conferences** - Company X video conferencing sessions must not be recorded unless this recording is approved in advance by the manager of information security and communicated in advance to all video conference participants.

**Logically Separate Voice And Data On IP Networks** - In every instance where voice over IP (VOIP) technology is deployed at Company X facilities, this technology must use a completely logically separate network other than the network used for data transmission.

**Critical Telephone Services Must Not Be Supported Via VOIP** - Company X business-critical telephone services -- such as over-the-phone order-taking with sales representatives -- must not be supported by voice over IP (VOIP) systems, until the Information Security Manager deems these systems sufficiently reliable and stable to support these services.

**VOIP Remote Management Or Auditing Requires Encrypted Channel** - Whenever either remote management or remote auditing is performed on a voice over IP (VOIP) network, these connections must employ a fully-encrypted channel.

**Direct Inward System Access Implementation** - Company X sites must not enable the direct inward system access features on private branch exchange telephone systems unless they are accompanied by a fraud detection and limitation system approved by the manager of the Telecommunications Department.

**Conference Bridge Activation** - Conference bridges must be specifically activated only when needed. They must not be left in an activated state when not in use.

### ****Internet and Intranet****

**Internet Transmission Of Sensitive Information** - Unencrypted Company X sensitive or private information must not be sent over the Internet.

**Publicly-Modifiable Directories** - All publicly-modifiable directories on Company X Internet-connected computers must be reviewed and cleared each evening.

**Internet News Sources** - News feeds, electronic mail mailing lists, push data updates, and other mechanisms for receiving information over the Internet must be restricted to material that is clearly related to Company X business and the duties of the receiving workers.

### ****Intranet Content****

**Intranet Postings** - Before any Confidential information is posted to the Company X intranet, both the department manager in charge of the relevant intranet page and the Owner of the involved information must approve.

**Intranet Content Ownership** - Unless approved in advance by the Information Technology Department Manager, and explicitly noted on the intranet web page, all content posted to the Company X intranet is the property of Company X.

### ****Web Site Security****

**Confidential Information On Web** – Company X Confidential information must not be resident on either Internet or intranet servers.

**Anonymous FTP Server Information** - All user-provided files that have not been explicitly approved for public release by the Marketing Department, and that are resident on the Company X anonymous FTP server, must be encrypted using Company X standard software.

**Internet Monitoring For Information Use** - The Legal Department must monitor the Internet on at least a monthly basis for the unauthorized use of Company X trademarks, service marks, brand names, or copyrighted materials owned by Company X.

### ****Public Information****

**Publicly Posting Only Generic Information** - With the exception of top management, all publicly-posted contact points must use generic job titles rather than individual names. For example, web sites, Internet public databases, and help wanted advertising would refer to "systems administrator" rather than "Mary Smith." Likewise, direct dial telephone numbers and individual email accounts must not be publicly posted.

**Permissible Ways To Obtain Competitive Information** - Company X workers must obtain information about competitors from public domain sources, or legally purchase such information from its rightful owner (such as a market research firm). Competitor information gathered by any other means, whether intentionally or unintentionally obtained must be reported immediately to the Company X senior management.

**Third-Party Use Of Organization Name** - No third-party organization may use the Company X name in its advertising or marketing materials unless the written permission of corporate legal counsel has first been obtained.

**Presentation Of Public Image** - Company X must at all-times present a low-profile and secure image to both the public and third parties. This means that information about the existence and nature of significant assets must be accessible only to those persons with a demonstrable need to know.

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

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

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 (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

CPL: 5.3. Information Exchange and Transit

HIPAA: Transmission Security 164.312(e)(1)

ISO/IEC 27002 - 13.2 Information transfer

NIST: SC-8 Transmission Integrity

PCI-DSS: 9.6.2 Media Transit Security

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 |  |
|  |  |  |  |  |