|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Customer Privacy Management Policy | | | | | |
| Policy # | CPL-16-02 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457847288)

[Scope 1](#_Toc457847289)

[Policy 1](#_Toc457847290)

[Privacy Policy Requirements 1](#_Toc457847291)

[Program Audit 2](#_Toc457847292)

[Collection Limitation 2](#_Toc457847293)

[Data Quality 2](#_Toc457847294)

[Purpose Specification 3](#_Toc457847295)

[Use Limitation 3](#_Toc457847296)

[Third Party Transfer 3](#_Toc457847297)

[Security Safeguards 4](#_Toc457847298)

[Openness 5](#_Toc457847299)

[Individual Participation 6](#_Toc457847300)

[Collecting Children’s Information 6](#_Toc457847301)

[Violations 6](#_Toc457847302)

[Definitions 6](#_Toc457847303)

[References 7](#_Toc457847304)

[Related Documents 7](#_Toc457847305)

[Approval and Ownership 7](#_Toc457847306)

[Revision History 7](#_Toc457847307)

Purpose

This policy establishes the responsibilities and minimum requirements for the implementation and maintenance of a privacy program at Company X. The privacy program is designed to protect all personally identifiable information of employees and customers against accidental disclosure.

Scope

This policy applies to all Company X information assets contained in any Company X facility and partner facilities. The target audience is Executive Management, IT Management, and the Board of Directors.

Policy

### ****Privacy Policy Requirements****

**Data Privacy Policies** – Company X will create and maintain written Data Privacy Policies that describe the ways in which sensitive customer information will be protected.

**Distribution Of Privacy Policies** - All internal Company X privacy policies that a prospect or a customer may need to know must be publicly posted or otherwise periodically distributed to these same people.

**Privacy Policy Reminder** - All Company X customers must be annually sent a copy of the Company X official privacy policy and instructions informing customers how they can opt out of Company X data sharing activities.

**Privacy Policy Change Notification** - Company X staff members must take reasonable steps to promptly notify all affected individuals whenever there has been a material change in documented privacy policies.

**Privacy Policy Differences Summary** - Company X must take reasonable steps to highlight key privacy policy differences when updates are distributed to affected individuals.

**Minimum Contents Of Posted Privacy Policy** - Every Company X privacy policy posted on the Internet at the very least must: describe how and when personal data is collected, explain how and when this personal data is used, notify data subjects when their data is transferred to third parties, offer data subjects an opportunity to "opt out" of transfers to third parties, describe relevant privacy and security measures, and explain the mechanisms for data subjects to change inaccurate personal data.

### **Program Audit**

**Privacy Policy And Practices Annual Audit** - In order to foster trust by Company X prospects and customers, each year Company X must be subjected to a privacy policy and practices audit conducted by an independent third party. The results of this audit must be posted on Company X's web site near the privacy policy.

### **Collection Limitation**

**Private Data Collection** - The collection of private data by Company X workers must be performed by lawful means, and only for a purpose related to the activities of Company X.

**Surreptitious Collection Of Private Information** - Company X computer and communications systems must not collect private data from customers or potential customers without having obtained their clear and unambiguous consent.

**Pretext Personal Data Collection** - Company X must not at any time gather personal information using misrepresentations or pretext statements about its right to receive such information.

**Private Data System Approval** - To be included in any Company X system that handles private data, the affected individuals must specifically elect to participate in the system.

**Biometric Information Collection** - Personal biometric information may not be captured by any Company X information systems unless the individual described has been previously notified of and has consented to the capture.

### **Data Quality**

**Correction, Deletion, And Blocking Of Inaccurate Personal Data** - Company X must provide data subjects with access to all personal information kept on file about them. In addition, Company X must provide these data subjects with mechanisms to correct, delete, or block the distribution to third parties, of personal information which is alleged to be inaccurate or outdated.

**Incorrect Personal Information** - Whenever Company X receives notice that certain personal information held in its records is incorrect, it must promptly modify the information, or else append to the record an indication that this information is disputed and alleged to be incorrect.

**Address Change Confirmation** - Customer requests to change a mailing address must be effective one month after the change has been entered into the system, and requests to change an electronic mail address will take place two business days after the change has been entered into the system, with both being confirmed by sending a notice to the previous address.

### ****Purpose Specification****

**Full And Accurate Description Of Private Data Collection** - Company X must provide its customers and prospects with a full and accurate description of all the private data captured as well as a clear description of how the data is used.

**Information Collection Notice** - In every instance where personally-identifiable information (PII) is collected; an explicit and understandable notice must be provided at the time and place the information is collected. Where information which is not personally-identifiable is collected, notice about this collection must nonetheless appear in the posted privacy policy.

**Identity Of Private Information Collector** - Both the collecting organization’s legal name and current contact information must be disclosed at each point where private information is collected. An exception will be made in those situations where this information can be easily determined from other information displayed on a user's screen.

**Private Information Requirement Explanation** - Whenever private information is requested by Company X information systems or workers, the full and complete reasons for collecting this information must also be disclosed. Furthermore, the consequences of a data subject's refusal to provide private information must also be disclosed at this point in time.

### ****Use Limitation****

**Personal Information For Business Functioning** - Company X must collect, process, store, and disseminate only that information that is necessary for the proper functioning of its business.

**Location-Specific Information Usage** - Company X currently has the ability to precisely locate those of its customers and/or employees who have laptop computer with wireless modems, wireless phones, personal digital assistants with wireless facilities, and other wireless smart devices. Company X will not use this information, or allow other commercial organizations to use this information, for marketing purposes unless specific authorization has been given by each such individual.

**Personal Data Uses After Merger Or Acquisition** - If Company X or any of its personal information collections are sold, merged, acquired, or otherwise transferred to another organization, such personal information may not be used for new and unanticipated purposes unless the involved individuals approve (opt-in to) these new uses.

### ****Third Party Transfer****

**When Private Data May Be Transferred To Third Parties** - Private information may be transferred to third parties only if (1) the data subject has been notified of, and agreed to the transfer, and (2) the third party agrees to be bound by the privacy policy in effect when the information was originally collected. Exceptions may be made when (1) an order regarding the transfer from a governmental agency such as a court of law has been received, (2) the data subject has submitted a written request for the transfer, or (3) the data subject has agreed to a new privacy policy that permits the transfer.

**Transferring Private Data** - Company X must release private data only to third-party organizations that commit in writing to maintain the information with an adequate level of protection, as determined by the Information Security Manager. Exceptions will be made in those cases where the release is required by law or regulation.

**Private Information Disclosure Records — Details** - Company X workers who release private information to third parties must keep records of all such disclosures including what information was disclosed, to whom it was disclosed, and the date of such disclosure.

**Private Information Disclosure Records — Maintenance** - Every disclosure of private information to third parties must be recorded and these records must be maintained for at least five years.

**Disclosure Of Private Information To Outsourcing Organizations** - Company X must not sell, rent, or otherwise transfer customer information to third parties in any manner unless the third parties sign a confidentiality agreement prohibiting them from further dissemination of this information and prohibiting them from using this information for unauthorized purposes.

**Transfer Of Customer Information After Business Change**- Company X may go out of business, merge, be acquired, or otherwise change the legal form of its organizational structure at some point in the future. Should such a change occur, Company X may need to share some or all of its customer information with another entity in order to continue to provide products and services. If such a change and associated information transfer takes place, customers will be promptly notified.

**Recording External Recipients Of Personal Information** - All people who have provided Company X with personal information have a right to know the identity of all third parties who have received their personal information. Upon receipt of a written request, the Chief Privacy Officer, or that officer's delegate, must provide data subjects with a complete list of all recipients of their information, including the nature of the information disclosed, and the dates of the disclosures.

**Private Data Movement To Third Party Custodians** - Movement of private data in the possession of Company X to a third party in all cases must involve the transfer of the data to a specific identified third party custodian. Before the third party custodian accepts such private data, he or she must agree to keep up-to-date records reflecting the names, addresses, and organizations of all other persons who will subsequently gain access to this same data.

### Security Safeguards

**Personal Information Access** - Access to any collection of personal information about potential customers and others with whom Company X has a business relationship must be strictly controlled on a need-to-know basis, and then used only for internal purposes. Unless clear and unambiguous consent of the party described in the information is first obtained, the information must not be sold, exchanged, or distributed to any third party.

**De-Identification Of Private Information** - Private information in the possession of Company X, which is no longer required in order to meet legal, regulatory, or business needs, must promptly be sanitized such that the identity of the individuals involved can no longer be linked to the data retained.

**Famous Customer Identifications** - Workers must not publicly acknowledge the identity of famous customers when in their presence unless the famous customers first openly state their names. Likewise, workers must refrain from talking about famous customers with anyone else other than Company X workers. An exception is made in those circumstance were workers need to reveal the identity of a famous customer in order to fill an order or to conduct other legitimate business activity. In these exceptional situations, workers must use a normal tone of voice and proceed in a normal businesslike manner.

**Private Information Access Logging** - For every production system containing information labeled as "private," access controls must be established such that every access to private information which initiated by a user is logged. These logs must show the individual whose information was accessed, the user requesting access, as well as the time and date.

**Embedded Personal Information** - Company X information systems must not employ secret serial numbers, secret personal identification numbers, or any other secret mechanisms that might reveal the identity of, or activities of customers.

**Personal Identifiers On Publicly-Accessible Locations** - Personal identifiers, such as social security numbers, must not appear on any publicly-accessible location managed by or controlled by Company X. This includes web pages, Internet commerce sites, product manuals, and magazine advertisements. An exception will be made for public encryption keys and digital certificates, both of which are intended to be widely available.

**Social Security Numbers Shown On Statements** - Social security numbers and other personal identifying information which the customer does not need to see must not be included in the statements or communications sent to customers. This policy applies whether statements or communications are sent via regular mail, electronic mail, or other methods.

**Account Number Intelligence** - In an effort to protect our customers against identity theft, Company X does not use externally-meaningful identifiers as its own internal customer account numbers. Thus, Company X customer account numbers must never be equivalent to social security numbers, driver's license numbers, or any other identifier which might be used in an unauthorized fashion by a third party.

**Examination Of Private User Files** - Systems administrators are authorized to examine private user files to handle emergencies other business needs (virus eradication, backup file restoration, etc.). Unless an investigation of alleged abusive or criminal acts is underway, whenever user files are examined in this manner, the involved user(s) must be promptly notified. After the problem has been resolved, all copies of such files made by the administrator must be promptly destroyed.

### ****Openness****

**Notice Of Privacy Practices Provided Before Consent Received** - All data subjects must be offered a notice about Company X's privacy practices, and must be given sufficient time to read and ask questions about these same practices, before they provide written consent allowing the use of their private data.

**Customer Access To Personal Information** - Customers have a right to obtain confirmation from Company X that personal information about them is kept on Company X systems. The nature of the information kept and the uses to which this information is put will generally be provided. If this cannot be done, the reasons why Company X has denied this request will nonetheless be promptly provided.

**Place No Software Or Information On User's Machine** - Company X does not place invisible software (such as spyware) or invisible information (such as persistent cookies) on the machine of any user who has visited either the Company X web or commerce site. Likewise, Company X does not in any way covertly change the software or information resident on the machines of these users.

### ****Individual Participation****

**Private Information Collection Consent** - Company X must obtain written consent from customers before it records any information about them in a computerized information system.

**Written Privacy Consent Needed For Provision Of Services** - Before any services are provided, customers must provide written consent to the disclosure of their private information to those Company X staff, and those authorized third parties, who need such access in order to perform the requested services. The involved local office manager has discretion to waive this requirement in the event of an emergency, or substantial barriers to communication, which prevents a customer from providing written consent.

**Opt-In For Sensitive Data And Opt-Out For Other Types** - Company X sensitive private data must not be shared with third parties unless the involved data subjects have first opted-in to this sharing process. On the other hand, non-sensitive private data may be shared with third parties consistent with Company X's privacy policy, so long as the data subjects have not previously opted-out.

**Revoking Data Usage Privileges** - If an individual or customer elects to revoke the permission that they gave Company X to use their personal data, Company X must promptly update its records and ensure that their wishes are observed.

### ****Collecting Children’s Information****

**Children’s Personal Information Collection** - Personal information about children must not be collected by any Company X information system without obtaining clear and unambiguous consent from the child’s parents or guardians.

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

**Opt-Out Notice** **-** Notification to customers that they may choose not to permit their information shared with nonaffiliated third parties.

**Pretext Calling** **-** A method of impersonation where a person poses as a customer or someone authorized to have customer information in order to obtain confidential customer data.

**Privacy Program** **-** The guidance provided that will enable Company X to maintain information about individuals while protecting the right of the individuals against unwarranted or illegal invasions of their privacy.

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

**Personally Identifiable Information (PII)** – Information that alone, or when combined with other personal or identifying information can be used to uniquely identify, contact, or locate a single person or can be used with other sources to uniquely identify a single individual.

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

References

CPL: 16.2 Customer Privacy Management

ISO 27002: 18.1.4 Privacy and protection of personally identifiable information

HIPAA: Privacy Rules

NIST: Appendix J: Privacy Controls

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 |  |
|  |  |  |  |  |