|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information Storage and Retention Policy | | | | | |
| Policy # | CPL-05-04 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Author | Phone | 888.641.0500 |

Table of Contents

[Purpose 1](#_Toc457915848)

[Scope 1](#_Toc457915849)

[Policy 1](#_Toc457915850)

[Information Collection 1](#_Toc457915851)

[Information Inventory 1](#_Toc457915852)

[Data Storage Restrictions 2](#_Toc457915853)

[Information Retention 2](#_Toc457915854)

[Litigation Hold 2](#_Toc457915855)

[Violations 2](#_Toc457915856)

[Definitions 3](#_Toc457915857)

[References 3](#_Toc457915858)

[Related Documents 3](#_Toc457915859)

[Approval and Ownership 3](#_Toc457915860)

[Revision History 3](#_Toc457915861)

Purpose

This policy establishes the minimum requirements for the inventory, retention and disposal of Company X internal and customer information.

Scope

This policy applies to all information resident on Company X computer systems and facilities, including those managed for Company X by third-parties.

Policy

### ****Information Collection****

**Information Collection** - When gathering information of a competitive or market intelligence nature, Company X staff, or third parties instructed to gather such information on behalf of Company X, must never lie or misrepresent their identity.

**Pretext Data Collection** – Company X staff or authorized third parties must not at any time gather personal information using misrepresentations or pretext statements about its right to receive such information.

### Information Inventory

**Asset Inventory - Information** - The Information Systems Department must compile and annually update a corporate-wide data dictionary and other high-level descriptions of the major Company X information assets. The data dictionary must include the specific Owners of this data.

**System of Record** - Each Owner must designate a system of record that will serve as the most authoritative copy of the information under his or her care. Updates to this information must be made to the system of record before or at the same time that updates are made to other systems containing this information.

### Data Storage Restrictions

**Storage Restrictions** – Sensitive data must always be encrypted during storage on electronic media:

**Encryption Standards** – All sensitive data encryption must follow standards established by the Information Technology Department.

### Information Retention

**Information Retention Periods** - A retention period must be assigned to all sensitive information, regardless of the form it takes (paper documents, computer files, etc.).

**Information Retention** - Information that is not specifically listed on the Information Retention Schedule must be retained only for as long as necessary, as designated by the information Owner.

**Customer Data Retention** – Customer data are retained and protected as long as each Customer continues to do business with Company X and for 90 days thereafter. At that point Company X may declassify or destroy customer data.

**Archival Storage Retention** - All financial accounting, tax accounting, and legal records must be retained for a period of at least seven years and all other business records must be retained for a period of at least five years.

**Record Destruction** - Workers must not destroy Company X sensitive information records unless these records appear on a list of records authorized for destruction.

### Litigation Hold

**Destroying Documents Relevant To Litigation** - If there is credible reason to believe that certain Company X internal documents may be needed as evidence in upcoming litigation, these documents must not be destroyed by the ongoing Company X document destruction process. They must instead be brought to the attention of internal legal counsel and then properly secured.

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

**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 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: 5.4 Information Storage and Retention

ISO/IEC 27002 - 18.1.3 Protection of records

HIPAA: Device and Media - Accountability (A)

PCI-DSS: PCI: R3. Protect stored cardholder data

Related Documents

Information Classification Policy

Information Destruction Policy

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 |  |
|  |  |  |  |  |