|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Information Security Policies | | | | | |
| Information Classification Policy | | | | | |
| Policy # | CPL-05-02 | Effective Date | MM/DD/YYYY | Email | policy@companyx.com |
| Version | 1.0 | Contact | Policy Contact | Phone | 888-641-0500 |

Table of Contents

[Purpose 1](#_Toc457915793)

[Scope 1](#_Toc457915794)

[Policy 1](#_Toc457915795)

[Asset Ownership 1](#_Toc457915796)

[Asset Classification 2](#_Toc457915797)

[Asset Labeling 2](#_Toc457915798)

[Declassification And Downgrading 3](#_Toc457915799)

[Violations 3](#_Toc457915800)

[Definitions 3](#_Toc457915801)

[References 4](#_Toc457915802)

[Related Documents 4](#_Toc457915803)

[Approval and Ownership 4](#_Toc457915804)

[Revision History 4](#_Toc457915805)

Purpose

This policy defines the requirements assigning and maintaining classification settings for all Company X computer and communications system information assets

Scope

This policy applies to all Company X computer systems and facilities, with a target audience of Company X Information Technology employees and partners.

Policy

### ****Asset Ownership****

**Information Ownership** - All production information possessed by or used by a particular organizational unit must have a designated Information Owner who is responsible for determining appropriate sensitivity classifications and criticality ratings, making decisions about who can access the information, and ensuring that appropriate controls are utilized in the storage, handling, distribution, and regular usage of information.

**Ownership Notice** - It is the responsibility of the chief information officer to ensure that this data dictionary includes a current indication of the Owners for all major Company X production information assets. It is the responsibility of all Owners to know the identity of the Custodians and users for the information types that have been entrusted to their care.

**Information Custodian** - Each significant type of production information must have a designated Custodian who will properly protect Company X information in keeping with the designated Information Owner’s access control, data sensitivity, and data criticality instructions.

**Information Systems Department Ownership Responsibility** - With the exception of operational computer and network information, the Information Systems Department must not be the Owner of any production business information.

### ****Asset Classification****

**Three-Category Data Classification** - All Company X data, including information entrusted to Company X from third parties, must be broken into the following three sensitivity classifications: CONFIDENTIAL, PRIVATE, and PUBLIC. Distinct handling, labeling, and review procedures must be established for each classification.

**Data Classification Descriptions** - The following descriptions are used for identifying and labeling each sensitivity classification for all Company X information.

**CONFIDENTIAL** - This classification label applies to highly sensitive business information that is intended for use only within Company X. Its unauthorized disclosure could adversely impact Company X or its customers, suppliers, business partners, or employees. Information that some people would consider to be private is included in this classification. Confidential Information may include, but is not limited to, confidential litigation documents, medical records, and attorney-client privilege documents.

**INTERNAL USE ONLY** **(PRIVATE)** - This information must be disclosed only to third parties if a confidentiality agreement has been signed. Disclosure is not expected to cause serious harm to Company X, and access is provided freely to all internal workers via the organization`s intranet. Examples include the organizational telephone book and staff automated calendars. This is the default classification for any information not specifically designated.

**PUBLIC** - This classification applies to information that has been approved by Company X management for release to the public. By definition, there is no such thing as unauthorized disclosure of this information and it may be disseminated without potential harm. Examples include product and service brochures, advertisements, job opening announcements, and press releases.

**Default Classification** - Information without a label is by default classified as Internal Use Only.

### ****Asset Labeling****

**Data Classification Labeling** - All confidential and private information must be labeled according to policies and standards issued by the Information Security Department, while information not falling into one or more of these categories need not be labeled.

**Assigning Data Classification Labels** - For all existing production information types, the Information Owner is responsible for choosing an appropriate data classification label to be used by all workers who create, compile, alter, or procure production information.

**Multiple Classification Labeling** - When information of various sensitivity classifications is combined, the resulting collection of information must be classified at the most restricted level found anywhere in the sources.

**Hardcopy Sensitivity Labels** - All printed, handwritten, or other human-readable manifestations of confidential or private information must have an appropriate sensitivity label on the upper-right corner of each page.

**Information Life Cycle Labeling** - From the time when information is created until it is destroyed or declassified, it must be labeled with a sensitivity designation if it is either secret, confidential, or private.

**Labels For Externally-Supplied Information** – All externally-provided information that is not clearly in the public domain must receive a Company X data classification system label. The Company X worker who receives this information is responsible for assigning an appropriate classification on behalf of the external party. When assigning a Company X classification label, this staff member must preserve copyright notices, author credits, guidelines for interpretation, and information about restricted dissemination.

### Declassification And Downgrading

**Dates For Reclassification** - If known, the date that Secret or Confidential information will no longer be sensitive or declassified must be indicated on all Company X sensitive information. This will assist those in possession of the information with its proper handling, even if these people have not been in recent communication with the information’s Owner.

**Expired Classification Labels** - Those workers in possession of sensitive information that was slated to be declassified on a date that has come and gone, but is not known definitively to have been declassified, must check with the information Owner before they disclose the information to any third parties.

**Notifications** - The designated information Owner may, at any time, declassify or downgrade the classification of information entrusted to his or her care. To achieve this, the Owner must change the classification label appearing on the original document, notify all known recipients and Custodians, and notify the Company X archives Custodian.

**Schedule For Review** - To determine whether sensitive information may be declassified or downgraded, at least once annually, information Owners must review the sensitivity classifications assigned to information for which they are responsible. From the standpoint of sensitivity, information must be declassified or downgraded as soon as practical.

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

**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.

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: 5.2. Information Classification

ISO/IEC 27002: 7.2.1 Classification Guidelines

ISO/IEC 27002: 7.2.2 Information Labeling and Handling

PCI-DSS: 9.6.1 Media Classification

NIST: MP-3 Media Marking

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 |  |
|  |  |  |  |  |