*Information Classification Policy*

Table of Contents

[Purpose 1](#_Toc525204989)

[Scope 1](#_Toc525204990)

[Policy 1](#_Toc525204991)

[Asset Ownership 1](#_Toc525204992)

[Asset Classification 2](#_Toc525204993)

[Asset Labeling 2](#_Toc525204994)

[Declassification And Downgrading 3](#_Toc525204995)

[Violations 3](#_Toc525204996)

[Definitions 4](#_Toc525204997)

[References 4](#_Toc525204998)

[Related Documents 4](#_Toc525204999)

[Approval and Ownership 4](#_Toc525205000)

[Revision History 5](#_Toc525205001)

Purpose

This policy defines the requirements assigning and maintaining classification settings for all CompanyX (the “Company”) **Information** system assets.

Scope

This policy applies to all CompanyX Information systems and facilities, with a target audience of CompanyX Information Technology employees and Third-Parties.

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.

**Information Custodian** - Each significant type of production information must have a designated Custodian who will properly protect CompanyX 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****

**Four-Category Data Classification** - All CompanyX data must be broken into the following four sensitivity classifications: SECRET, CONFIDENTIAL, PRIVATE, and UNCLASSIFIED. 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 CompanyX information.

**SECRET** - This classification label applies to the most sensitive business information that is intended for use strictly within CompanyX. Its unauthorized disclosure could seriously and adversely impact CompanyX, its customers, its business Third-Parties, and its suppliers. Examples include merger and acquisition documents, corporate level strategic plans, litigation strategy memos, reports on breakthrough new product research, and Trade Secrets such as certain computer programs.

**CONFIDENTIAL** - This classification label applies to less-sensitive business information that is intended for use within CompanyX. Its unauthorized disclosure could adversely impact CompanyX or its customers, suppliers, business Third-Parties, or employees. Information that some people would consider to be private is included in this classification. Examples include employee performance evaluations, customer transaction data, strategic alliance agreements, unpublished internally-generated market research, computer passwords, and internal audit reports.

**PRIVATE - FOR INTERNAL USE ONLY** - This classification label applies to all other information that does not clearly fit into the previous two classifications. While its unauthorized disclosure is against policy, it is not expected to seriously or adversely impact CompanyX or its employees, suppliers, business Third-Parties, or its customers. Examples include the CompanyX telephone directory, dial-up computer access numbers, new employee training materials, and internal policy manuals.

**PUBLIC** - This classification applies to information that has been approved by CompanyX 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****

**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.

**Data Classification Labeling** - All secret, 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.

**Equipment Identification Codes** - All CompanyX **Information** equipment must have an identification number permanently etched onto the equipment that can be used to assist police in their attempts to return stolen property.

**Hardcopy Sensitivity Labels** - All printed, handwritten, or other human-readable manifestations of secret, 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** - With the exception of general business correspondence and copyrighted software, all externally-provided information that is not clearly in the public domain must receive a CompanyX data classification system label. The CompanyX worker who receives this information is responsible for assigning an appropriate classification on behalf of the external party. When assigning a CompanyX 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 CompanyX 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 CompanyX 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. CompanyX reserves the right to notify the appropriate law enforcement authorities of any unlawful activity and to cooperate in any investigation of such activity. CompanyX does not consider conduct in violation of this policy to be within an employee’s or Third-Party’s course and scope of employment, or the direct consequence of the discharge of the employee’s or Third-Party’s duties. Accordingly, to the extent permitted by law, CompanyX reserves the right not to defend or pay any damages awarded against employees or Third-Parties that result from violation of this policy.

Any employee or contractor who is requested to undertake an activity which he or she believes is in violation of this policy, must provide a written or verbal complaint to his or her manager, any other manager or the Human Resources Department as soon as possible.

Definitions

Confidential Information (Sensitive Information) – Any CompanyX 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 CompanyX from a Third-Party under a non-disclosure agreement

**Information Asset** - Any CompanyX data in any form, and the equipment used to manage, process, or store CompanyX data, that is used in the course of executing business. This includes, but is not limited to, corporate, customer, and Third-Party data.

Third-Party – Any non-employee of CompanyX who is contractually bound to provide some form of service to CompanyX.

**User -** Any CompanyX employee or Third-Party who has been authorized to access any CompanyX electronic information resource.

References

ISO/IEC 27002: 7.2.1 Classification Guidelines

PCI-DSS: 9.6.1 Media Classification

NIST: MP-3 Media Marking

US-CSF: ID.AM-5: Resource classification

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 | 10/05/2019 | MM/DD/YYYY |  |
|  |  |  |  |  |